H3C MSR
Open Multiservice Routerシリーズ
Comware 7 SSL VPN設定ガイド

New H3C Technologies, co., ltd
http://www.h3c.com
ソフトウェアバージョン:R6728
ドキュメントバージョン:6 W 100-20230510

商標

New H3C Technologies Co.,Ltd.の商標を除き、本書に記載されているすべての商標は、それぞれの所有者の所有物です。

お知らせ

本書に記載されている情報は、予告なしに変更されることがあります。本書の記述、情報、推奨事項を含むすべての内容は正確であると考えられますが、明示的または黙示的を問わず、いかなる種類の保証もなく提示されています。H3Cは、本書に含まれる技術的または編集上の誤りや脱落に対して責任を負いません。

内容

SSL VPNの設定

SSL VPNの概要

SSL VPNは、SSL VPNゲートウェイを介してSSLベースのセキュアなリモートアクセスサービスを提供します。インターネット上のどこからでも、ユーザーはSSL対応ブラウザを介してSSL VPNゲートウェイへのセキュアな接続を確立し、ゲートウェイの背後にある保護されたリソースにアクセスできます。

SSL VPNの動作メカニズム

SSL VPNゲートウェイの背後にある保護されたリソースへのリモートユーザークセスを許可するには、これらのリソースをゲートウェイ上で設定する必要があります。リモートユーザーは、ゲートウェイへのSSL暗号化接続を確立し、ID認証を通過した後に、許可されたリソースにだけアクセスできます。

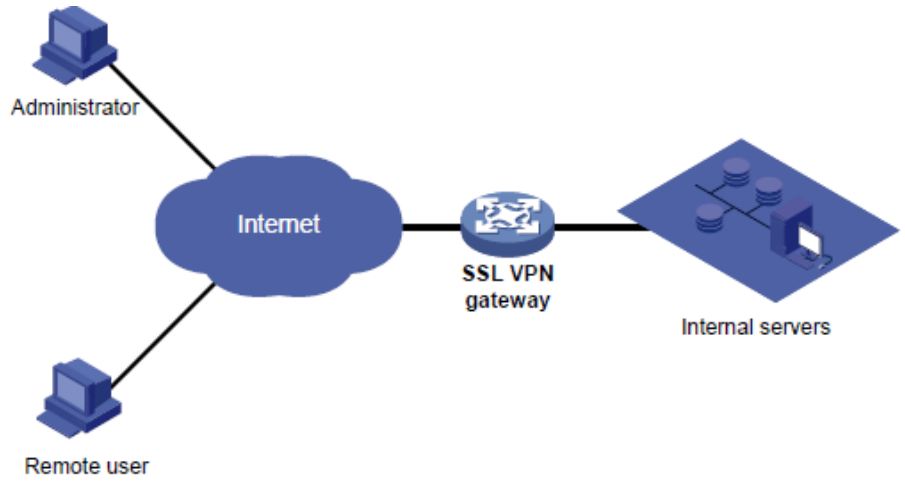
図1に示すように、SSL VPNは次のように動作します。

1. リモートユーザーは、SSL VPNゲートウェイへのHTTPS接続を確立します。

   このプロセスでは、リモートユーザーとSSL VPNゲートウェイがSSL証明書認証を実行します。
2. リモートユーザーは、ユーザー名とパスワードを入力します。
3. SSL VPNゲートウェイは、ユーザーが入力したクレデンシャルを認証し、ユーザーに一連のリソースへのアクセスを許可します。
4. ユーザーは、アクセスするリソースを選択します。

   そのリソースに対するアクセス要求は、SSL接続を介してSSL VPNゲートウェイに送信されます。
5. SSL VPNゲートウェイは要求を解決し、対応する内部サーバーに要求を転送します。
6. SSL VPNゲートウェイは、SSL接続を介してサーバーの応答をユーザーに転送します。

図1 SSL VPNネットワークダイアグラム

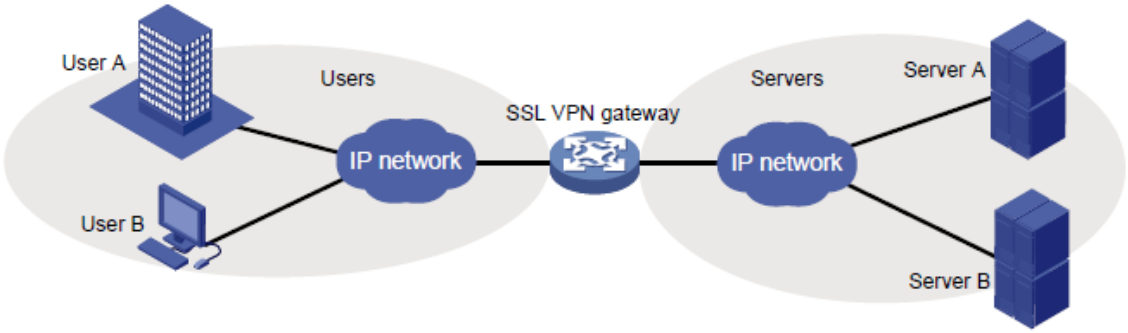


SSL VPNネットワーキングモード

ゲートウェイモード

ゲートウェイモードでは、図2に示すように、SSL VPNゲートウェイはリモートユーザーと内部サーバーネットワークを接続するゲートウェイとして機能します。SSL VPNゲートウェイはインラインで配置されるため、内部ネットワークを完全に保護できますが、データ伝送のパフォーマンスに影響を与えます。

図2 ゲートウェイモード

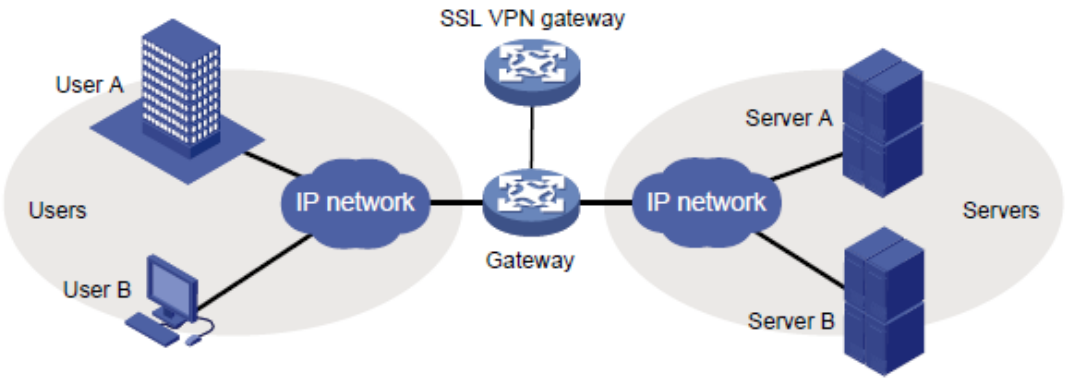


シングルアームモード

シングルアームモードでは、図3に示すように、SSL VPNゲートウェイがネットワークゲートウェイに接続されます。

ゲートウェイは、ユーザーからサーバーへのトラフィックをSSL VPNゲートウェイに転送します。SSL VPNゲートウェイはトラフィックを処理し、処理されたトラフィックをゲートウェイに送り返します。ゲートウェイは、トラフィックを内部サーバーに転送します。SSL VPNゲートウェイは、キーパスに展開されないため、ネットワークのパフォーマンスのボトルネックにはなりません。ただし、SSL VPNゲートウェイは、内部ネットワークに対して完全な保護を提供できません。

図3 シングルアームモード



SSL VPNアクセスモード

Webアクセス

Webアクセスモードでは、リモートユーザーはブラウザを使用して、HTTPSを介してSSL VPNゲートウェイによって許可されたWebリソースにアクセスします。ログイン後、ユーザーはWebページにリストされている任意のリソースにアクセスできます。Webアクセスモードでは、すべての操作がWebページで実行されます。

SSL VPN Webアクセスユーザーが使用できるリソースは、Webサーバーだけです。

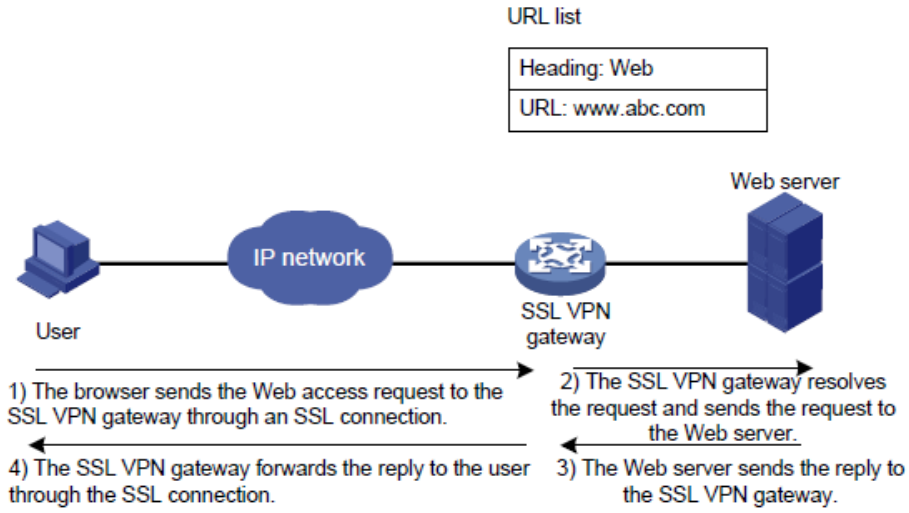
Webアクセスを実装するには、SSL VPNゲートウェイでURLのリストを設定する必要があります。URLは、内部WebサーバーのIPアドレスまたはドメイン名です。

Webアクセスの手順は次のとおりです。

1. ユーザーはブラウザを使用して、HTTPS経由でSSL VPNゲートウェイにログインします。
2. SSL VPNゲートウェイはユーザーを認証し、使用可能なURLへのアクセスをユーザーに許可します。
   認可されたURLは、SSL VPNゲートウェイWebページにURLリンクとして表示されます。
3. ユーザーは、SSL VPNゲートウェイWebページでアクセスするURLを選択します。ブラウザは、HTTPS用のSSL接続を介してSSL VPNゲートウェイにアクセス要求を送信します。
4. SSL VPNゲートウェイは要求を解決し、HTTPまたはHTTPSを使用してWebサーバーに要求を送信します。
5. Webサーバーから応答を受信した後、SSL VPNゲートウェイはHTTPS用のSSL接続を介してユーザーに応答を転送します。

図4は、Webアクセスプロセスを示しています。管理者がSSL VPNゲートウェイにwww.h3c.comのURLを設定します。次に、SSL VPNユーザーは、SSL VPNゲートウェイWebページのURLにアクセスすることで、内部Webサーバーにアクセスできます。

図4 Webアクセスのネットワークダイアグラム



TCPアクセス

TCPアクセスモードでは、ユーザーはアプリケーションのオープンポートにアクセスすることで、内部サーバー上のTCPアプリケーションにアクセスします。サポートされるアプリケーションには、リモートアクセスサービス(Telnetなど)、デスクトップ共有サービス、メールサービス、Notesサービス、および固定ポートを使用するその他のTCPサービスが含まれます。

TCPアクセスモードでは、ユーザーはSSL VPNクライアント(ユーザーが使用する端末デバイス)にTCPア

クセスクライアントソフトウェアをインストールします。クライアントソフトウェアは、SSL接続を使用してアプリケーション層データを送信します。

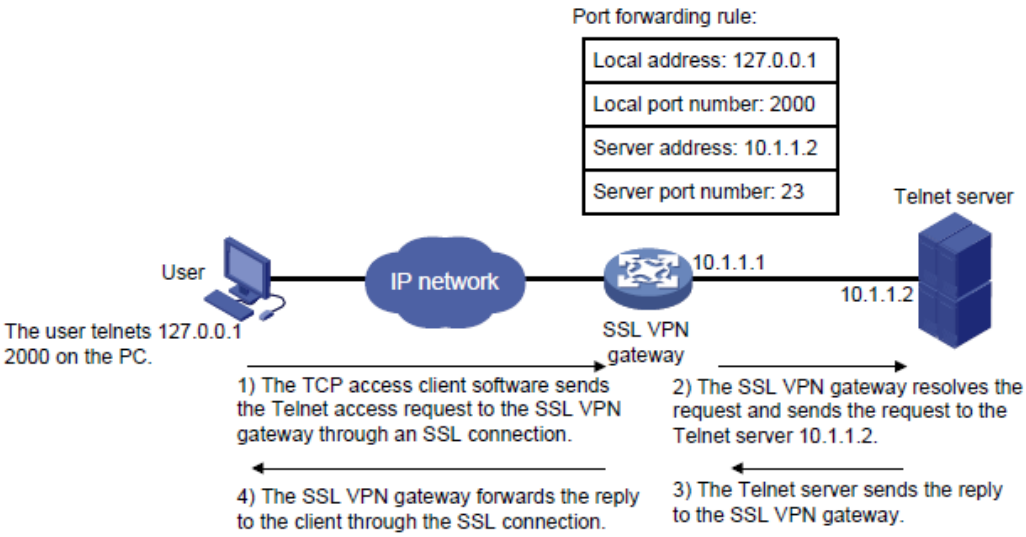
TCPアクセスを実装するには、SSL VPNゲートウェイでポート転送インスタンスを設定する必要があります。ポート転送インスタンスは、TCPサービス(IPアドレス/ドメイン名およびポート番号で識別)をSSL VPNクライアントのローカルIPアドレス(またはホスト名)およびポート番号にマッピングします。

TCPアクセス手順は、次のとおりです。

1. ユーザーはブラウザを使用して、HTTPS経由でSSL VPNゲートウェイにログインします。
2. SSL VPNゲートウェイはユーザーを認証し、Telnetサービス(ポート転送インスタンス)へのアクセスをユーザーに許可します。
3. ユーザーは、SSL VPNゲートウェイのWebページからTCPアクセスクライアントソフトウェアをダウンロードし、ソフトウェアを起動します。ソフトウェアは、ポート転送インスタンスで許可されたローカルポートを開きます。
4. ユーザーはローカルIPアドレスとポート番号にアクセスしようとします。TCPアクセスクライアントソフトウェアは、SSL接続を介してSSL VPNゲートウェイにアクセス要求を送信します。
5. SSL VPNゲートウェイは要求を解決し、ポート転送インスタンスに従ってTelnetサーバーに要求を送信します。
6. Telnetサーバーから応答を受信した後、SSL VPNゲートウェイはSSL接続を介してユーザーに応答を転送します。

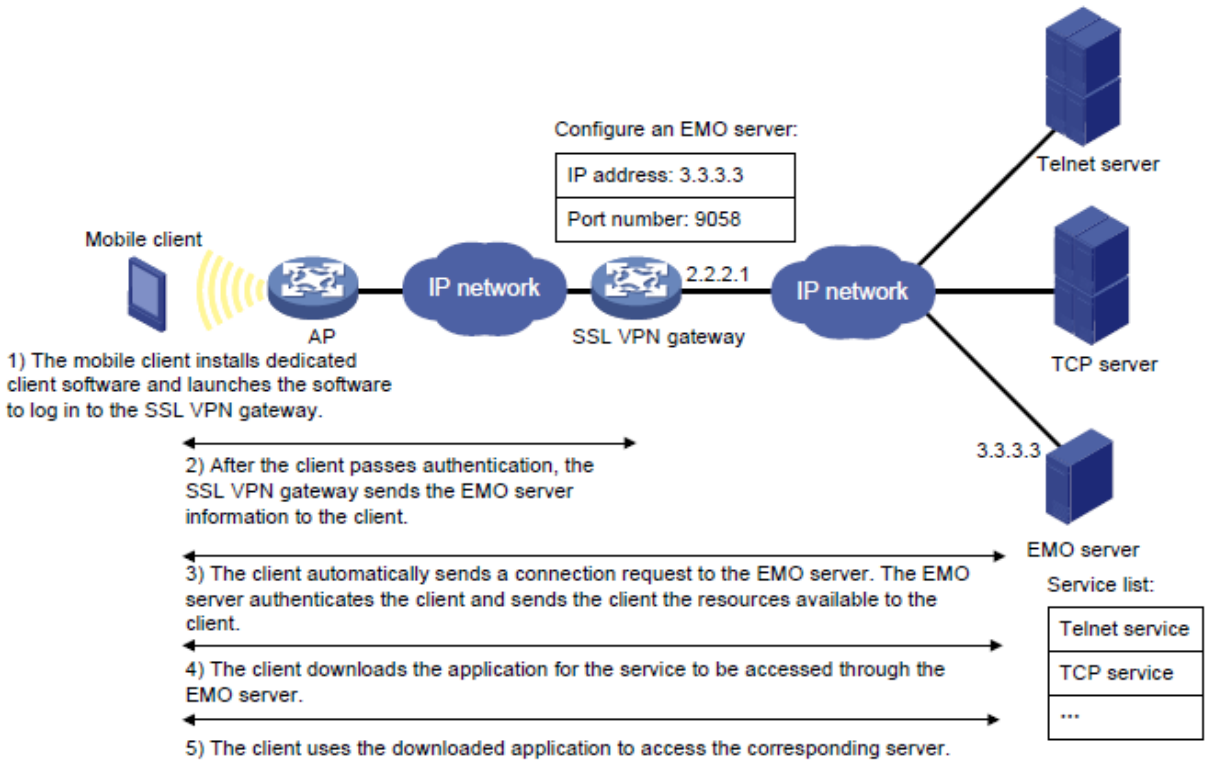
図5に示すように、管理者はSSL VPNゲートウェイ上にTelnetサービスのポート転送インスタンスを作成します。ルールは、内部Telnetサーバーのアドレス10.1.1.2とポート番号23を、SSL VPNクライアントのローカルアドレス127.0.0.1とローカルポート番号2000にマッピングします。次に、SSL VPNユーザーは、ローカルアドレス127.0.0.1とローカルポート番号2000をtelnetすることによって、内部Telnetサーバーにアクセスできます。

図5 TCPアクセスのネットワークダイアグラム



モバイルクライアントでTCPアクセスモードを使用する場合、SSL VPNゲートウェイでポート転送インスタンスを設定する必要はありません。ただし、モバイルクライアント専用のクライアントソフトウェアが必要であり、SSL VPNゲートウェイでモバイルクライアント用のEndpoint Mobile Office(EMO)サーバーを指定する必要があります。モバイルクライアントは、EMOサーバーを介して内部リソースにアクセスします。図6は、アクセスプロセスを示しています。

図6 モバイルクライアントから内部サーバーへのアクセスのネットワークダイアグラム



IPアクセス

IPアクセスは、リモートユーザーと内部サーバー間にセキュアなIP通信を実装します。

IPアクセスモードで内部サーバーにアクセスするには、専用のIPアクセスクライアントソフトウェアをインストールする必要があります。クライアントソフトウェアは、SSL VPNクライアントにVirtual Network Interface Card(VNIC;仮想ネットワークインターフェースカード)をインストールします。

IPアクセスを実装するには、SSL VPNゲートウェイで次の項目を設定する必要があります。

- SSL VPN ACインターフェース。
- アクセス可能なIPリソースへのルート。ルートは、パケット転送を指示するためにSSL VPNクライアントに発行されます。

図7では、IPアクセスプロセスを説明するためにping操作を使用しています。管理者はまず、SSL VPNゲートウェイでpingの宛先(サーバー10.1.1.2/24)へのルートを設定する必要があります。

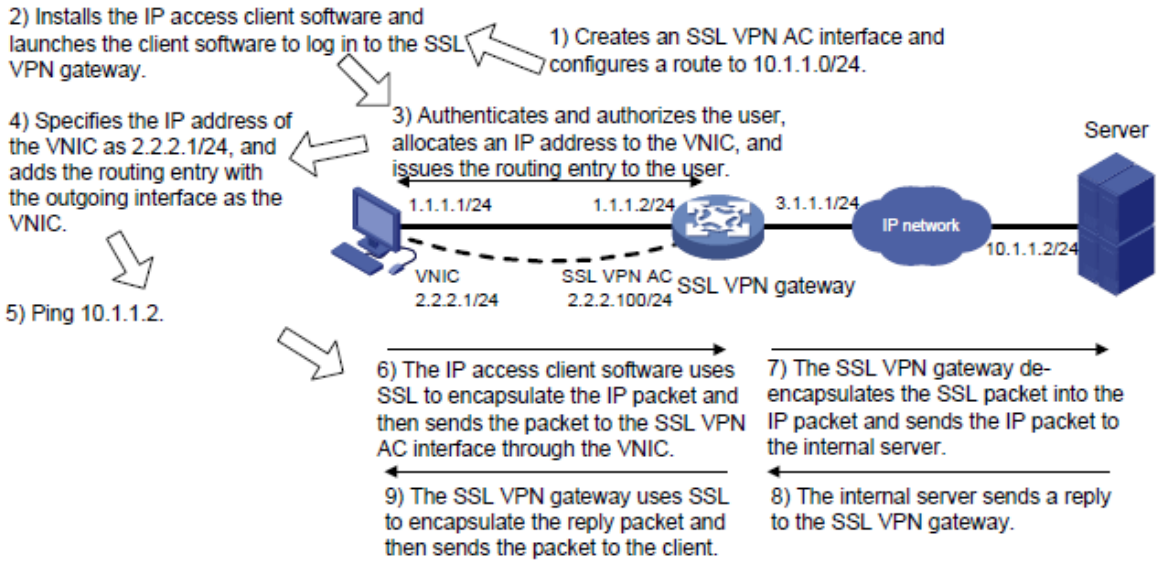
アクセスプロセスは次のとおりです。

1. ユーザーは、IPアクセスクライアントソフトウェアをインストールし、クライアントソフトウェアを起動してSSL VPNゲートウェイにログインします。
2. SSL VPNゲートウェイは、次の操作を実行します。
   a. ユーザーを認証および認可します。
   b. ユーザーのVNICにIPアドレスを割り当てます。
   c. 認可されたIPアクセスリソースをクライアントに発行します。この例では、サーバー10.1.1.2/24へのルートが発行されます。
3. クライアントは、割り当てられた IP アドレスを VNIC のアドレスとして指定し、VNIC を出力インターフェイスとして使用してルートをローカル ルーティング テーブルに追加します。
4. ユーザーがサーバーアドレスにpingを実行します。

   ping要求はルートと一致します。一致するパケットはSSLによってカプセル化されます。

5. クライアントはSSLを使用してping要求パケットをカプセル化し、VNICを介してSSL VPN ACインターフェースにパケットを送信します。
6. SSL VPNゲートウェイは、SSLパケットをIPパケットにカプセル化解除し、そのIPパケットを対応する内部サーバーに転送します。
7. 内部サーバーは、SSL VPNゲートウェイに応答を送信します。
8. SSL VPNゲートウェイは、SSLを使用して応答パケットをカプセル化し、SSL VPN ACインターフェースを介してクライアントにパケットを送信します。

図7 IPアクセスのネットワークダイアグラム



SSL VPNユーザー認証

SSL VPNコンテキスト内のリソースにアクセスするには、ユーザーはまずSSL VPNコンテキストにログインするためにID認証を渡す必要があります。SSL VPNコンテキストの認証方式には、ユーザー名/パスワード認証、証明書認証、確認コード認証、SMS認証、およびカスタム認証があります。SMS認証とカスタム認証の両方がイネーブルの場合、カスタム認証だけが有効になります。

SSL VPNコンテキストでは、ユーザー名/パスワード認証、証明書認証、またはその両方をイネーブルにできます。SSL VPNコンテキストへのログインにこれらの認証方式が必要かどうかは、authentication useコマンドの設定によって異なります。ユーザーに対してユーザー名/パスワード認証を使用するには、AAAでユーザーのアカウントも作成する必要があります。詳細については、「AAAの設定」を参照してください。

また、SSL VPNコンテキストで検証コード認証、SMS認証、およびカスタム認証をイネーブルにすることもできます。これらの認証方式は、設定されている場合、ログイン認証に必要です。

ユーザー名/パスワード認証

ユーザー名/パスワード認証プロセスは、次のとおりです。

1. SSL VPNユーザーは、SSL VPNログインページでログインユーザー名とパスワードを入力します。ユーザー名とパスワードはSSL VPNゲートウェイに送信されます。
2. SSL VPNゲートウェイは、受信したユーザー名とパスワードをAAAに送信して認証、認可、アカウンティングを行うか、カスタム認証サーバーに送信して認証と認可を行います。

証明書の認証

図8に示すように、証明書認証プロセスは次のとおりです。

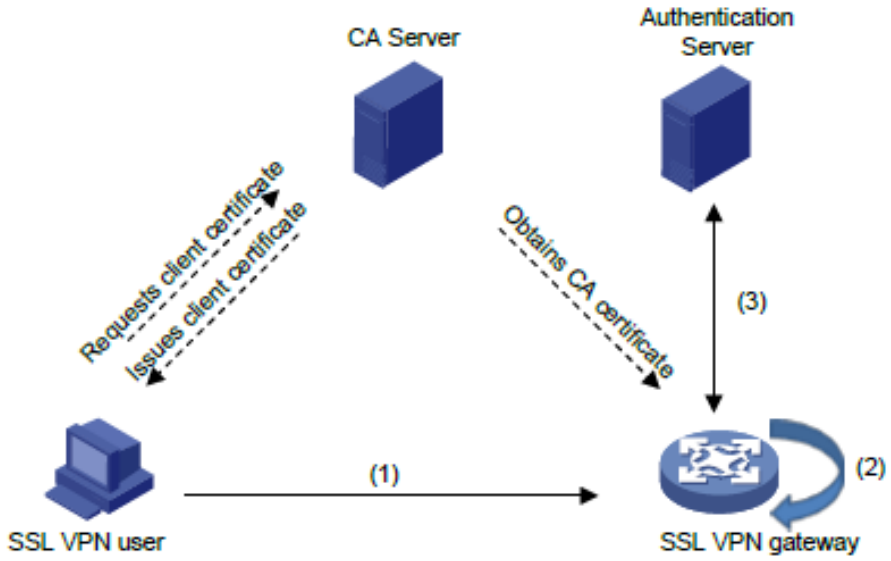
1. SSL VPNユーザーは、プロンプトが表示されたときにログイン用の証明書を選択します。証明書は、SSL接続要求でSSL VPNゲートウェイに送信されます。
2. SSL VPNゲートウェイは、ユーザー証明書の有効性を確認します。
   - 証明書が無効であると確認された場合、ゲートウェイはSSL接続要求を拒否します。ユーザーはSSL VPNコンテキストにログインできません。
   - 証明書が有効であることが確認されると、SSL接続が確立され、ゲートウェイは次の手順を実行します。
3. CRLチェックがイネーブルになっている場合、SSL VPNゲートウェイは証明書失効をチェックします。
   - 証明書が失効していないことが確認されると、SSL接続が確立され、ゲートウェイは次の手順を実行します。
   - 証明書が失効していることが確認されると、ゲートウェイはSSL接続要求を拒否します。ユーザーはSSL VPNコンテキストにログインできません。

   CRLチェックの詳細については、「PKIの設定」を参照してください。
4. SSL VPNゲートウェイは、証明書アトリビュート(デフォルトではCNアトリビュート)からユーザー名を抽出します。次に、SSL VPNゲートウェイは、認可およびアカウンティングのためにユーザー名をAAAに送信するか、認可のためにカスタム認証サーバーに送信します。

注:

証明書認証を使用するには、指定した証明書アトリビュートから抽出されたユーザー名が認証サーバーに存在することを確認します。

図8 証明書認証プロセス



ユーザー名/パスワード認証と証明書認証の組み合わせ

ユーザー名/パスワードの複合認証と証明書認証の認証プロセスは、次のとおりです。

1. SSL VPNユーザーは、プロンプトが表示されたときにログイン用の証明書を選択します。証明書は、SSL接続要求でSSL VPNゲートウェイに送信されます。
2. SSL VPNゲートウェイは、ユーザー証明書の有効性を確認します。
   - 証明書が無効であると確認された場合、ゲートウェイはSSL接続要求を拒否します。ユーザーはSSL VPNコンテキストにログインできません。
   - 証明書が有効であることが確認されると、SSL接続が確立され、ゲートウェイは次の手順を

実行します。

3. CRLチェックがイネーブルになっている場合、SSL VPNゲートウェイは証明書失効をチェックします。
   - 証明書が失効していないことが確認されると、SSL接続が確立され、ゲートウェイは次の手順を実行します。
   - 証明書が失効していることが確認されると、ゲートウェイはSSL接続要求を拒否します。ユーザーはSSL VPNコンテキストにログインできません。
4. SSL VPNゲートウェイは、証明書からユーザー名を抽出し、抽出されたユーザー名をユーザーが指定したユーザー名と比較します。
   - 2つのユーザー名が一致する場合、ユーザーはID認証を通過します。次に、SSL VPNゲートウェイは、認証、認可、アカウンティングのためにユーザー名とパスワードをAAAに送信するか、認証と認可のためにカスタム認証サーバーに送信します。
   - 2つのユーザー名が一致しない場合、ユーザーはID認証に失敗します。

注:

ユーザーは、アクセスモードに応じて、証明書を選択するとき、またはSSL接続が確立された後に、ユーザー名とパスワードを入力する場合があります。

SMS認証

SMS認証をイネーブルにすると、デバイスはSMS検証コードを使用してSSL VPNユーザーを認証します。ユーザーがSSL VPNゲートウェイにログインできるのは、ユーザーがSMS認証に合格した場合だけです。

デバイスは、次のタイプのSMS認証をサポートしています。

- IMC SMS認証。

  SSL VPNユーザーのSMS認証は、IMCサーバーによって実行されます。IMC SMS認証ビューで、IMCサーバーのIPアドレスとポート番号を設定する必要があります。
- SMSゲートウェイ認証。

  SSL VPNユーザーのSMSゲートウェイ認証は、SMSゲートウェイによって実行されます。SMSゲートウェイ認証ビューで、SMSゲートウェイ、検証コードの再送間隔、および検証コードの有効期間を指定する必要があります。

2つのSMS認証タイプの両方を設定することはできません。

SMSゲートウェイ認証では、1つのユーザー名を1つの携帯電話番号にのみバインドできます。複数のユーザーが同じユーザー名を使用してSSL VPNゲートウェイにログインする場合、ユーザーは検証コードの受信順序を確認する必要があります。ユーザーは、受信した検証コードを自分のログイン試行に対して送信する必要があります。

カスタム認証

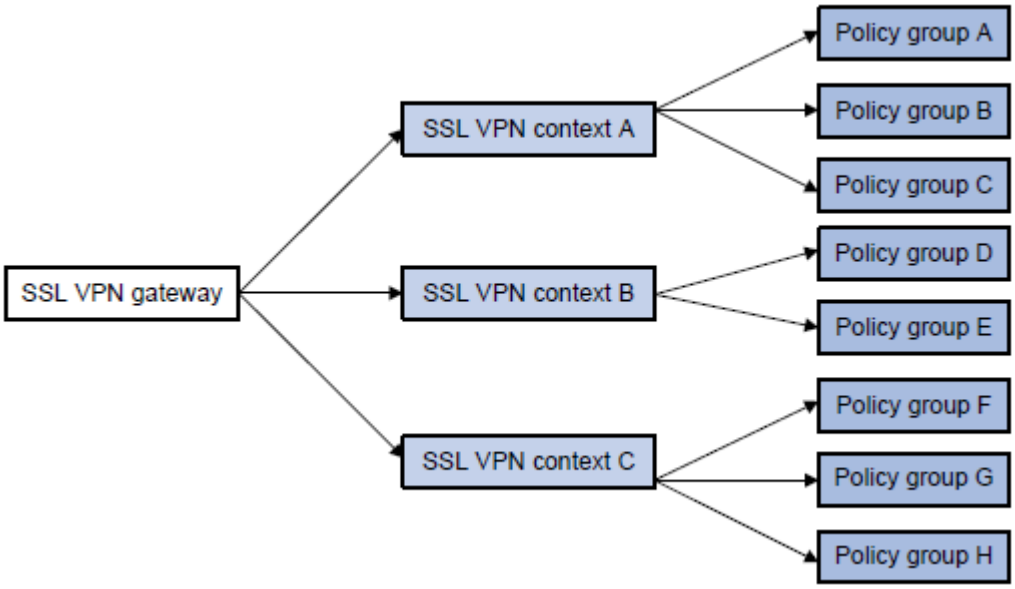
カスタム認証を使用すると、必要に応じてカスタム認証サーバーを設定できます。デバイスは、カスタム認証サーバーを使用してユーザーの認証と認可を行うことができます。カスタム認証サーバーはアカウンティングをサポートしていません。

リソースアクセス制御

SSL VPNは、ユーザー単位でリソースへのユーザークセスを制御します。

図9に示すように、SSL VPNゲートウェイは複数のSSL VPNコンテキストに関連付けることができます。SSL VPNコンテキストには、複数のポリシーグループが含まれます。ポリシーグループは、アクセス可能なWebリソース、TCPリソース、およびIPリソースを定義します。

図9 SSL VPNリソースアクセスコントロール



SSL VPNゲートウェイに関連付けられたSSL VPNコンテキストのドメイン名または仮想ホスト名を指定できます。ユーザーがSSL VPNゲートウェイにログインすると、SSL VPNゲートウェイは次の操作を実行します。

1. ユーザーが入力したドメイン名または仮想ホスト名を使用して、ユーザーが属するSSL VPNコンテキストを決定します。
2. コンテキストに指定されたISPドメインの認証方式と認可方式を使用して、ユーザーの認証と認可を実行します。
   - SSL VPNゲートウェイがユーザーにポリシーグループの使用を許可した場合、ユーザーはポリシーグループによって許可されたリソースにアクセスできます。
   - SSL VPNゲートウェイがユーザーにポリシーグループの使用を許可しない場合、ユーザーはデフォルトポリシーグループで許可されているリソースにアクセスできます。

注:

SSL VPNゲートウェイは、AAAサーバーまたはカスタム認証サーバーを使用して、ユーザーの認証および認可を実行します。SSL VPNは、AAAプロトコルRADIUSおよびLDAPをサポートします。RADIUSが最もよく使用されます。

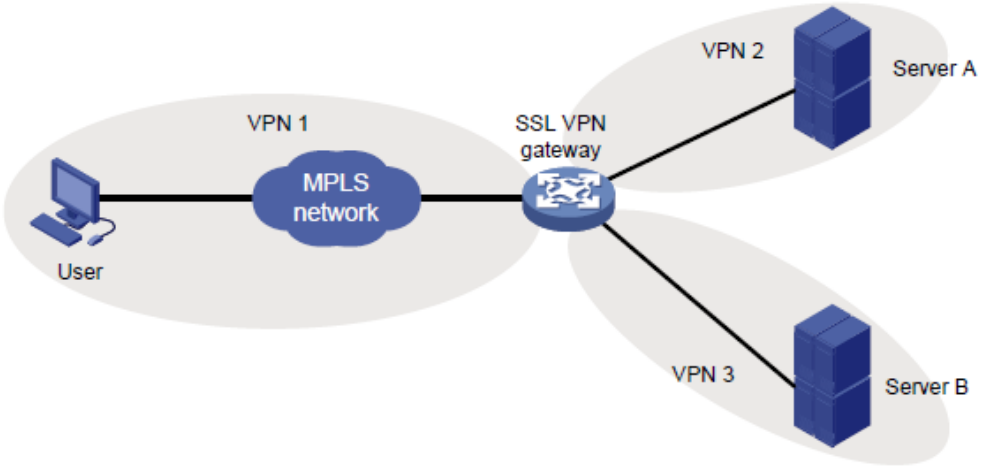
VRF対応SSL VPN

VRF対応SSL VPNは、次の機能を提供します。

- VRF対応SSL VPNコンテキスト:SSL VPNゲートウェイ上で、異なるSSL VPNコンテキストを異なるVRFインスタンス(VPNインスタンス)に関連付けます。SSL VPNコンテキスト内のユーザーは、SSL VPNコンテキストに関連付けられたVPNインスタンス内のリソースだけにアクセスできます。VRF対応SSL VPNコンテキストでは、サーバードレスのオーバーラップも許可されます。
- VRF対応SSL VPNゲートウェイ:SSL VPNゲートウェイが属するVPNインスタンスを指定します。SSL VPNゲートウェイにアクセスできるのは、同じVPN内のユーザーだけです。VRF対応SSL VPNゲートウェイは、内部サーバーリソースがパブリックネットワークまたは他のVPNに漏れるのを防ぎます。

VPNインスタンスの詳細については、『MPLS Configuration Guide』の「MPLS L3VPN」を参照してください。

図10 VRF 対応 SSL VPN



制約事項:SSL VPNとのハードウェア互換性

ハードウェア	SSL VPNの互換性
MSR810、MSR810-W、MSR810-W-DB、MSR810-LM、MSR810-W-LM、MSR810-10-PoE、MSR810-LM-HK MSR810-W-LM-HK、MSR810-LM-CNDE-SJK、MSR810-CNDE-SJK	はい
MSR810-LMS、MSR810-LUS	いいえ
MSR810-LMS-EA、MSR810-LME	はい
MSR1004S-5G	はい
MSR2600-6-X1、MSR2600-10-X1、MSR2600-15-X1	はい
MSR 2630	はい
MSR3600-28 and MSR3600-51	はい
MSR3600-28-SI、MSR3600-51-SI	いいえ
MSR3600-28-X1、MSR3600-28-X1-DP、MSR3600-51-X1、MSR3600-51-X1-DP	はい
MSR3610-I-DP、MSR3610-IE-DP、MSR3610-IE-ES、MSR3610-IE-EAD、MSR-EAD-AK770、MSR3610-I-IG、MSR3610-IE-IG	はい
MSR3610-X1、MSR3610-X1-DP、MSR3610-X1-DC、MSR3610-X1-DP-DC、MSR3620-X1、MSR3640-X1	はい
MSR 3610、MSR 3620、MSR 3620-DP、MSR 3640、MSR 3660	はい
MSR3610-G、MSR3620-G	はい
MSR 3640-X 1-HI	はい

ハードウェア	SSL VPNの互換性
MSR810-W-WiNet、MSR810-LM-WiNe	はい
MSR830-4LM-WiNet	はい

MSR830-5BEI-WiNet、MSR830-6EI-WiNet、MSR830-10BEI-WiNet	はい
MSR830-6BHI-WiNet、MSR830-10BHI-WiNet	はい
MSR2600-6-WiNet、MSR2600-10-X1-WiNet	はい
MSR2630-WiNet	はい
MSR 3600-28- WiNet	はい
MSR3610-X1-WiNet	はい
MSR3610-WiNet、MSR3620-10-WiNet、MSR3620-DP-WiNet、MSR3620-WiNet、MSR3660-WiNet	はい

ハードウェア	SSL VPNの互換性
MSR2630-XS	はい
MSR3600-28-XS	はい
MSR3610-XS	はい
MSR3620-XS	はい
MSR3610-I-XS	はい
MSR3610-IE-XS	はい
MSR3620-X1-XS	はい
MSR3640-XS	はい
MSR3660-XS	はい

ハードウェア	SSL VPNの互換性
MSR810-LM-GL	はい
MSR810-W-LM-GL	はい
MSR830-6EI-GL	はい
MSR830-10EI-GL	はい
MSR830-6HI-GL	はい
MSR830-10HI-GL	はい
MSR1004S-5G-GL	はい
MSR2600-6-X1-GL	はい
MSR3600-28-SI-GL	いいえ

制約事項:SSL VPNのライセンス要件

デフォルトでは、SSL VPNゲートウェイは最大15のオンラインユーザーカウントをサポートします。

ライセンスを購入してインストールすると、サポートされるオンラインユーザーの数を増やすことができます。ライセンスの詳細は、『Fundamentals Configuration Guide』の「license management」を参照してください。

IRFファブリックでサポートされるオンラインユーザーの最大数は、次のように計算されます。

IRFファブリックでサポートされる最大オンラインユーザー数=各メンバーデバイスのライセンスで許可される最大オンラインユーザー数の合計+デフォルトでサポートされる最大オンラインユーザー数。

メンバーデバイスに障害が発生した後、そのライセンスはIRFファブリックで60日間有効になります。

制約事項およびガイドライン:SSL VPNの設定

SSL VPNゲートウェイは、次の方法でWebリソースとIPリソースの両方にアクセスするユーザーに対して、セッションを1つだけ生成します。

1. まず、ユーザーはWebブラウザを介してSSL VPNゲートウェイにアクセスします。
2. 次に、ユーザーは、Webページを介してIPアクセスクライアントをダウンロードし、IPアクセスクライアントを起動する。

ユーザーがWebブラウザまたはIPアクセスクライアントを終了すると、セッションは終了し、ユーザーはWebリソースにもIPアクセスリソースにもアクセスできなくなります。

SSL VPNポリシーグループで、ユーザーアクセスフィルタリング用のACLを指定できます。指定したACLのルールにVPN設定が含まれている場合、そのルールは有効になりません。

SSL VPNタスクの概要

SSL VPNを設定するには、SSL VPNゲートウェイで次の作業を実行します。

1. SSL VPNゲートウェイの設定
2. SSL VPNコンテキストの設定
3. SSL VPNユーザー認証、認可、およびアカウンティングの設定
   a. SSL VPNコンテキストでのユーザー認証の設定
   b. SSL VPNユーザー認証サーバーの設定

      カスタム認証サーバーは、カスタム認証用に構成する必要があります。
4. 必要に応じたSSL VPNリソースアクセスコントロールの設定
   - URI ACLの設定
   - Webアクセスサービスを構成する
   - TCPアクセスサービスの設定
   - IPアクセスサービスの設定
   - モバイルクライアントのSSL VPNアクセスの設定
   - (省略可能)ショートカットの構成
   - (省略可能)リダイレクトリソースの構成
   - (オプション)HTTPリダイレクションの設定
   - (任意)SSL VPNコンテキストのデフォルトポリシーグループの設定
5. (任意)VRF-aware SSL VPNの設定
   - SSL VPNコンテキストとVPNインスタンスの関連付け
   - SSL VPNゲートウェイのVPNインスタンスの指定

      6. (任意)SSL VPNユーザー制御の設定
   - オンラインSSL VPNユーザー制御の設定

- SSL VPNセッションレート制限の設定
- SSL VPNクラッキング防止の設定
- SSL VPN SSOログインの設定

- 拒否されたSSL VPNクライアントタイプの設定
- (任意)SSL VPN Webページのカスタマイズ
  SSL VPN Webページ要素のカスタマイズ
- SSL VPN Webページテンプレートの指定

7. (任意)SSL VPNロギングのイネーブル化

SSL VPNの前提条件

SSL VPNゲートウェイを設定する前に、次の作業を完了します。

- PKIを設定し、SSL VPNゲートウェイのデジタル証明書を取得します(「PKIの設定」を参照)。
- SSL VPNゲートウェイで使用するSSLサーバーポリシーを設定します(「SSLの設定」を参照)。

SSL VPNゲートウェイの設定

制限事項およびガイドライン

デフォルトのIPv4またはIPv6アドレスを使用するSSL VPNゲートウェイでは、HTTPSサービスポート番号とは異なるポート番号を使用する必要があります。

SSL VPNゲートウェイに適用されるSSLサーバーポリシーの設定が変更された場合、変更されたポリシーを使用するには、SSL VPNゲートウェイをいったんディセーブルにしてからイネーブルにする必要があります。

SSL VPNゲートウェイのIPアドレスとポート番号の両方を、デバイス上のHTTPSサーバーのIPアドレスおよびポート番号と同じにすることはできません。同じにしないと、SSL VPN Webインターフェースだけにアクセスできますが、これらのIPアドレスとポート番号を使用してデバイス管理Webインターフェースにアクセスすることはできません。

手順

1. システムビューに入ります。

   system-view
2. SSL VPNゲートウェイを作成し、そのビューを入力します。

   sslvpn gateway *gateway-name*
3. SSL VPNゲートウェイのIPv4アドレスとポート番号を設定します。

   ip address *ip-address* [**port** *port-number*]

   デフォルトでは、SSL VPNゲートウェイはIPv4アドレス0.0.0.0とポート番号443を使用します。

   ポート番号を指定せずにip addressコマンドを設定すると、デフォルトのポート番号(443)が使用されます。
4. SSLサーバーポリシーをSSL VPNゲートウェイに適用します。

   ip address *ip-address* [**port** *port-number*]

   デフォルトでは、SSL VPNゲートウェイは自己署名証明書のSSLサーバーポリシーを使用します。
5. SSL VPNゲートウェイをイネーブルにします。

service enable

デフォルトでは、SSL VPNゲートウェイはディセーブルになっています。

SSL VPNコンテキストの設定

このタスクについて

SSL VPNコンテキストは、ユーザーセッションとユーザーが使用できるリソースを管理します。

制限事項およびガイドライン

SSL VPNコンテキストをSSL VPNゲートウェイに関連付ける場合は、次の注意事項に従ってください。

- コンテキストのドメイン名または仮想ホスト名が、SSL VPNゲートウェイに関連付けられている既存のコンテキストと異なることを確認します。
- コンテキストのドメイン名または仮想ホスト名を指定しない場合、他のSSL VPNコンテキストをSSL VPNゲートウェイに関連付けることはできません。
- 仮想ホスト名を指定する場合は、ネットワークにDNSサーバーを展開して、仮想ホスト名をSSL VPNゲートウェイのIPアドレスに解決します。

SSL VPNコンテキストは、最大10のSSL VPNゲートウェイに関連付けることができます。

手順

1. システムビューに入ります。

   system-view
2. SSL VPNコンテキストを作成し、そのビューを開始します。

   sslvpn context *context-name*
3. コンテキストをSSL VPNゲートウェイに関連付けます。
   gateway *gateway-name* [**domain** *domain-name* | **virtual-host** virtual-host-name *]*

   デフォルトでは、コンテキストはSSL VPNゲートウェイに関連付けられていません。
4. コンテキスト内のSSL VPNユーザーのAAAのISPドメインを指定します。

   aaa domain *domain-name*

   デフォルトでは、SSL VPNコンテキスト内のSSL VPNユーザーのAAAには、デフォルトのISPドメインが使用されます。

   SSL VPNユーザー名は、ISPドメイン情報を伝送できません。このコマンドが実行されると、SSL VPNゲートウェイは、コンテキスト内のSSL VPNユーザーのAAAに指定されたドメインを使用します。
5. コンテキストを有効にします。

   service enable

   デフォルトでは、コンテキストはディセーブルです。
6. (任意)コンテキストのセッション(オンラインユーザー)の最大数を設定します。

   max-users *max-number*

   デフォルトでは、SSL VPNコンテキストは最大1048575セッション(オンラインユーザー)をサポートします。
7. (任意)SSL VPNセッションのアイドルタイムアウトタイマーを設定します。

   timeout idle *minutes*

デフォルトでは、SSL VPNセッションのアイドルタイムアウトタイマーは30分です。

8. (任意)SSL VPNセッションのアイドルカットトラフィックのしきい値を設定します。

   idle-cut traffic-threshold

   デフォルトでは、SSL VPNセッションのアイドルカットトラフィックのしきい値は0バイトです。timeout idleコマンドで指定されたセッションアイドルタイムアウト時間内にトラフィックが送信されない場合、SSL VPNセッションは切断されます。

9. (任意)SSLクライアントポリシーをSSL VPNコンテキストに適用します。

   ssl client-policy *policy-name*

   非FIPSモードの場合:

   SSL VPNのデフォルトのSSLクライアントポリシーが使用されます。このポリシーは、**dhe_rsa_aes_128_cbc_sha**, **dhe_rsa_aes_256_cbc_sha**, **rsa_3des_ede_cbc_sha**, **rsa_aes_128_cbc_sha**, and **rsa_aes_256_cbc_sha**暗号スイートをサポートします。

   FIPSモードの場合:

   SSL VPNのデフォルトのSSLクライアントポリシーが使用されます。このポリシーは **rsa_aes_128_cbc_sha** and **rsa_aes_256_cbc_sha** cipher suites暗号スイート。

   SSL VPNゲートウェイは、指定されたSSLクライアントポリシーの設定を使用してHTTPSサーバーに接続します。

10. (任意)URLマスキングをグローバルにイネーブルにします。

    url-masking enable

    URLマスキングは、デフォルトで無効になっています。

    URLマスキングがイネーブルになると、SSL VPNコンテキストで設定されたWebアクセスリソースのURLがコード化された文字列に変換されます。

SSL VPNコンテキストでのユーザー認証の設定

SSL VPNコンテキストでのユーザー認証設定の制約事項およびガイドライン

証明書認証の動作は、SSLサーバーポリシービューのclient-verifyコマンドの設定によって異なります。このコマンドを使用して、必須またはオプションのSSLクライアント認証をイネーブルにできます。必須証明書認証は、WebユーザーおよびIPアクセスユーザーに対してだけサポートされます。TCPアクセスユーザーおよびモバイルクライアントユーザーがSSL VPNゲートウェイに正常にアクセスするには、オプションのSSLクライアント認証を使用する必要があります。

ユーザー認証タスクの概要

SSL VPNコンテキストでユーザー認証を設定するには、次のタスクを実行します。

1. ユーザーログインに必要な認証方式の指定
2. 基本認証方式の設定
   - ユーザー名/パスワード認証の構成
   - 証明書認証の設定
3. (オプション)検証コード認証の設定

4. (オプション)IMC SMS認証の設定
5. (オプション)SMSゲートウェイ認証の設定
6. (省略可能)ユーザーのパスワード変更の構成

ユーザーログインに必要な認証方式の指定

このタスクについて

SSL VPNコンテキストでは、ユーザー名/パスワード認証、証明書認証、またはその両方をイネーブルにできます。SSL VPNコンテキストへのログインにこれらの認証方式が必要かどうかは、authentication use allコマンドの設定によって異なります。

- authentication use allコマンドが設定されている場合、ユーザーはログイン用にイネーブルになっているすべての認証方式に合格する必要があります。
- authentication use any-oneコマンドが設定されている場合、ユーザーはイネーブルになっている任意の認証方式を通過した後にログインできます。

手順

1. システムビューに入ります。
   system-view
2. SSL VPNコンテキストビューを開始します。
   sslvpn context *context-name*
3. ユーザーログインに必要な認証方式を指定します。
   authentication use **{** all **|** any-one }
   デフォルトでは、ユーザーはSSL VPNコンテキストにログインするために、イネーブルになっているすべての認証方式を渡す必要があります。

ユーザー名/パスワード認証の構成

1. システムビューに入ります。
   システムビュー
2. SSL VPNコンテキストビューを開始します。
   sslvpn context *context-name*
3. ユーザー名/パスワード認証をイネーブルにします。
   password-authentication enable
   ユーザー名/パスワード認証は、デフォルトでイネーブルになっています。

証明書認証の設定

1. システムビューに入ります。
   system-view
2. SSL VPNコンテキストビューを開始します。
   sslvpn context *context-name*
3. 証明書認証を有効にします。

certificate-authentication enable

証明書認証は、デフォルトでは無効になっています。

4. 証明書アトリビュートをSSL VPNユーザー名として指定します。

   certificate username-attribute { **cn** | **email-prefix** | **oid** *extern-id* }

   デフォルトでは、デバイスは証明書のサブジェクトのCNアトリビュートの値をSSL VPNユーザー名として使用します。

検証コード認証の設定

1. システムビューに入ります。

   system-view

2. SSL VPNコンテキストビューを開始します。

   sslvpn context *context-name*

3. 検証コード認証を有効にします。

   verify-code enable

   デフォルトでは、検証コード認証はイネーブルになっています。

IMC SMS認証の設定

1. システムビューに入ります。

   system-view

2. SSL VPNコンテキストビューを開始します。

   sslvpn context *context-name*

3. IMC SMS認証をイネーブルにします。

   sms-auth type imc

   デフォルトでは、IMC SMS認証はディセーブルになっています。

4. IMC SMS認証ビューを作成して入力します。

   sms-auth imc

5. IMCサーバーを指定します。

   server-address *ip-address* **port** *port-number* [**vpn-instance** *vpn-instance-name*]

   デフォルトでは、IMCサーバーは指定されていません。

SMSゲートウェイ認証の設定

前提条件

SMSゲートウェイの構成を完了します。SMSゲートウェイの構成の詳細は、「SMSの構成」を参照してください。

手順

1. システムビューに入ります。

   system-view

2. SSL VPNコンテキストビューを開始します。

sslvpn context *context-name*

3. SSL VPNユーザービューを開始します。

   user *username*

4. SMSメッセージを受信するSSL VPNユーザーの携帯番号を指定します。

   mobile-num *number*

   デフォルトでは、SMSメッセージを受信するための携帯電話番号は指定されていません。

5. SSL VPNコンテキストビューに戻ります。

   quit

6. SMSゲートウェイ認証をイネーブルにします。

   sms-auth type sms-gw

   デフォルトでは、SMSゲートウェイ認証はディセーブルになっています。

7. SMSゲートウェイ認証ビューを作成して開始します。

   sms-auth sms-gw

   デフォルトでは、SMSゲートウェイ認証ビューは存在しません。

8. SMSゲートウェイを指定します。

   gateway *sms-gateway-name*

   デフォルトでは、SMSゲートウェイは指定されていません。

9. 携帯電話番号のバインドを有効にします。

   mobile-num-binding enable

   デフォルトでは、モバイル番号バインディングはディセーブルになっています。

10. 確認コードの再送間隔を設定します。

    verification-code send-interval ***seconds***

    デフォルトでは、確認コードの再送信間隔は60秒です。

11. 検証コードの有効期間を設定します。

    verification-code validity *minutes*

    デフォルトでは、検証コードの有効期間は1分です。

12. 携帯電話の国番号を指定します。

    country-code *country-code*

    既定では、携帯電話の国番号は86です。

13. SMSコンテンツテンプレートを設定します。

    sms-content *string*

    デフォルトでは、SMSコンテンツテンプレートは**Hello, $$USER$$**で、確認コードは$$VERIFYCODE$$で、有効期間は分単位で$$VALIDTIME$$です。

ユーザーのパスワード変更の構成

このタスクについて

パスワード変更を使用すると、SSL VPNユーザーは、SSL VPN Webインターフェースにログインした後に、個人設定ページでログインパスワードを変更できます。この機能は、IMC認証ユーザーだけで使用できます。

この機能をディセーブルにすると、パスワード変更機能がSSL VPN Webインターフェースに表示されなくな

り、ユーザーがパスワードを変更できなくなります。

手順

1. システムビューに入ります。
   system-view
2. SSL VPNコンテキストビューを開始します。
   sslvpn context *context-name*
3. SSL VPNコンテキストのSSL VPNユーザーがパスワードを変更できるようにします。
   password-changing enable
   デフォルトでは、SSL VPNコンテキスト内のSSL VPNユーザーは、パスワードを変更できます。
4. SSL VPNユーザービューを開始します。
   user *username*
5. (任意)SSL VPNユーザーのパスワード変更をイネーブルにします。
   password-changing enable
   デフォルトでは、SSL VPNユーザーはパスワードを変更できます。
6. パスワード変更用のIMCサーバーを指定します。
   self-service imc address *ip-address* **port** *port-number* [**vpn-instance** *vpn-instance-name*]
   デフォルトでは、パスワードの変更にIMCサーバーは指定されていません。
   このコマンドは、IMC認証ユーザーがSSL VPNログインパスワードを変更する必要がある場合にだけ実行します。

SSL VPNユーザー認証サーバーの設定

SSL VPNユーザー認証サーバータイプの指定

このタスクについて

SSL VPNユーザー認証では、次のタイプのサーバーがサポートされます。

- **AAA認証サーバー**: デバイスは、ユーザーの認証、認可、アカウンティングにAAAサーバーを使用します。AAAの詳細については、「AAAの設定」を参照してください。
- **カスタム認証サーバー**: 必要に応じて、カスタム認証サーバーを設定できます。デバイスは、ユーザーの認証および認可にカスタム認証サーバーを使用できます。カスタム認証サーバーはアカウンティングをサポートしていません。カスタム認証サーバーの設定の詳細については、「カスタム認証サーバーの設定」を参照してください。

手順

1. システムビューに入ります。
   system-view
2. SSL VPNコンテキストビューを開始します。
   sslvpn context *context-na*
3. 認証サーバーのタイプを指定します。
   authentication server-type **{** aaa **|** custom **}**

デフォルトでは、SSL VPN認証サーバーはAAAサーバーです。

カスタム認証サーバーの構成

このタスクについて

ユーザーの認証および認可にカスタム認証サーバーを使用するには、次の設定を行います。

- カスタム認証サーバーのURL。

  SSL VPNゲートウェイは、HTTPを使用して、指定されたURLに認証要求を送信します。
- カスタム認証タイムアウト。

  SSL VPNゲートウェイは、HTTP要求をカスタム認証サーバーに送信した後、サーバーからの応答を待機します。ゲートウェイが認証タイムアウト内に応答を受信しない場合、SSL VPNクライアントに認証失敗メッセージを返します。
- カスタム認証用のHTTP要求設定。

  SSL VPNゲートウェイは、HTTP要求方式、要求ヘッダーフィールド、要求テンプレートなどの認証要求設定に基づいて、HTTP要求を構築します。
- カスタム認証用のHTTP応答設定。

  SSL VPNゲートウェイは、認証応答設定に基づいてHTTP応答を解析します。設定には、HTTP応答形式、応答内の認証成功値、応答内のフィールド名、およびカスタム形式のHTTP応答の応答テンプレートが含まれます。

手順

1. システムビューに入ります。

   system-view
2. SSL VPNコンテキストビューを開始します。

   sslvpn context *context-name*
3. カスタム認証サーバーのURLを設定します。

   custom-authentication url ***url***

   デフォルトでは、カスタム認証サーバーのURLは設定されていません。
4. カスタム認証タイムアウトを指定します。

   custom-authentication timeout ***seconds***

   デフォルトでは、カスタム認証のタイムアウトは15秒です。
5. カスタム認証要求の設定を構成します。
   a. HTTP要求方式を設定します。

      custom-authentication request-method **{** get **|** post **}**

      デフォルトでは、HTTP要求メソッドはGETです。
   b. HTTP要求ヘッダーフィールドを設定します。

      custom-authentication request-header-field *field-name* **value** *value*

      デフォルトでは、カスタム認証要求ヘッダーには次のフィールドが含まれます。
      - **Content-type:application/x-www-form-urlencoded**
      - **User-Agent:nodejs 4.1.**
      - **Accept:text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q**
   c. HTTP要求テンプレートを設定します。

custom-authentication request-template ***template***

デフォルトでは、要求テンプレートは設定されていません。

6. カスタム認証応答の設定を構成します。
   a. HTTP応答形式を指定します。

      custom-authentication response-format **{** custom **|** json **|** xml **}**

      デフォルトでは、HTTPレスポンスのフォーマットはJSONです。

   b. HTTP応答の認証成功値を設定します。

      custom-authentication response-success-value *success-value*

      デフォルトでは、HTTP応答に認証成功値は設定されていません。

   c. HTTP応答のフィールド名を設定します。
      custom-authentication response-field { **group** *group* | **message** *message* | result *result* }

      デフォルトでは、HTTP応答フィールド名は設定されていません。

      HTTP応答フォーマットがJSONまたはXMLの場合は、HTTP応答フィールド名を設定する必要があります。

   d. カスタム形式のHTTP応答のフィールドの応答テンプレートを設定します。
      custom-authentication response-custom-template { **group** | **message** | result } *template*

      デフォルトでは、応答テンプレートは設定されていません。

      応答テンプレートは、HTTP応答形式がカスタムの場合に必要です。

URI ACLの設定

このタスクについて

URI ACLは、リソースへのアクセスを許可または拒否する一連の規則です。URI ACLを使用して、SSL VPNユーザーのIP、TCP、およびWebアクセスを細かくフィルタリングできます。

1つのURI ACLに複数のルールを追加できます。デバイスは、ルールIDの昇順でパケットをルールと照合します。一致するルールが見つかると、照合プロセスは停止します。

SSL VPNコンテキストでは、複数のURI ACLを作成できます。

URI ACLは、次のフィールドに基づいて、SSL VPNユーザーのHTTP、HTTPS、TCP、UDP、ICMP、およびIPトラフィックをフィルタリングできます。

- プロトコルタイプ。
- IPアドレス。
- ホスト名。
- ポート番号。
- URL。

手順

1. システムビューに入ります。

   system-view

2. SSL VPNコンテキストビューを開始します。

sslvpn context *context-name*

3. URI ACLを作成し、そのビューを入力します。

   uri-acl *uri-acl-name*

4. URI ACLにルールを設定します。

   rule [*rule-id*] { **deny** | **permit** } **uri** *uri-pattern-string*

   デフォルトでは、URI ACLにルールは設定されていません。

Webアクセスサービスを構成する

リモートユーザーがWebアクセスモードで内部リソースにアクセスできるようにするには、Webアクセスリソースを設定し、そのリソースをSSL VPNポリシーグループに関連付ける必要があります。

Webアクセスサービスタスクの概要

Webアクセスサービスを構成するには、次のタスクを実行します。

1. URLリストの設定
2. Webアクセス用のSSL VPNポリシーグループの設定
3. (省略可能)ファイルポリシーの構成

URLリストの設定

このタスクについて

URLリストは、SSL VPNゲートウェイの背後にあるアクセス可能なWebリソースを定義するURL項目のリストです。各URL項目は、内部Webリソースに対応します。

SSL VPNゲートウェイは、要求しているユーザーにURLを送信する前に、内部サーバーから返されたリソースURLを書き換えます。URLマッピングタイプによって、ゲートウェイがURLを書き換える方法が決まります。

次の例では、ユーザーがURL **http://www.server.com:8080**で内部リソースにアクセスする場合のURLマッピングの動作について説明します。SSL VPNゲートウェイ名は**gw**、ドメインネームは**https://www.gateway.com:4430**, 、IPアドレスは**1.1.1.1**です。

- **通常の書き換え**: 既定のマッピング方法です。クライアントに返されるリソースURLは、**https://www.gateway.com:4430/_proxy2/http/8080/www.server.com**に書き換えられます。
- **ドメインマッピング**: クライアントに返されるリソースURLは、**https**://mapped domain name:**4430**に書き換えられます。mapped domain nameは、ユーザー定義のドメインネームです。
- **ポートマッピング**: ポートマッピングの仮想ホスト名の有無にかかわらず、ゲートウェイ名を指定できます。次に例を示します。
  - ゲートウェイ名として**gw2**を指定し、仮想ホスト名を指定しない場合、リソースURLは**https://2.2.2.2:4430**, に書き換えられます。ここで、2.2.2.2と4430はSSL VPNゲートウェイgw2のIPアドレスとポート番号です。
  - ゲートウェイ名に**gw**、仮想ホスト名に**vhosta**を指定した場合、リソースURLはhttps://vhosta:4430に書き換えられます。

制限事項およびガイドライン

リソースURLの書き換えは、HTML、XML、CSS、またはJavaScriptファイルを含むリソースアクセス応答に対してのみ使用できます。

通常の書き換えでは、URLの書き換えの失敗や書き換えエラーなどの問題が発生し、SSL VPNクライアントが内部リソースにアクセスできなくなる可能性があります。ドメインマッピングまたはURLマッピングを使用することをお勧めします。

手順

1. システムビューに入ります。
   system-view
2. SSL VPNコンテキストビューを開始します。
   sslvpn context *context-name*
3. URLアイテムを作成し、そのビューを入力します。
   url-item *name*
4. URL項目にリソースURLを指定します。
   url *url*
   デフォルトでは、URL項目にリソースURLは指定されていません。
   リソースURLでプロトコルタイプを指定しない場合、デフォルトのプロトコル(HTTP)が使用されます。
5. (任意)URLマスキングをイネーブルにします。
   url-masking enable
   デフォルトでは、URLマスキングは無効になっています。
   URLマスキングが有効になると、URL項目のWebリソースURLがコード化された文字列に変換されます。
6. (任意)URL項目にURI ACLを指定します。
   resources uri-acl *uri-acl-name*
   デフォルトでは、URI ACLは指定されていません。
7. (任意)URLマッピング方式を設定します。
   url-mapping{ **domain-mapping** *domain-name*| **port-mapping gateway** *gateway-name*[**virtual-host** *virtual-host-name*] } [**rewrite-enable**]
   デフォルトでは、通常の書き換え方法が使用されます。
8. SSL VPNコンテキストビューに戻ります。
   quit
9. URLリストを作成し、そのビューを入力します。
   url-list *name*
10. (任意)URLリストの見出しを設定します。
    heading *string*
    デフォルトでは、URLリストの見出しはWebです。
11. URL項目をURLリストに追加します。
    resources url-item ***name***
    デフォルトでは、URLリストにURL項目は含まれていません。

Webアクセス用のSSL VPNポリシーグループの設定

このタスクについて

Webアクセス用のSSL VPNポリシーグループを設定するには、URLリストをポリシーグループに関連付けます。認証サーバーがユーザーにポリシーグループの使用を許可すると、ユーザーはポリシーグループに関連付けられたURLリストによって提供されるWebリソースにアクセスできます。

ポリシーグループでは、詳細ACLおよびURI ACLを指定して、ユーザーのWebアクセス要求をフィルタリングできます。

詳細ACLは、宛先IPアドレスおよび宛先ポート番号によるWebアクセス要求のフィルタリングをサポートしています。URI ACLは、プロトコルタイプ、宛先アドレス、ドメイン名、ポート番号およびURLによるWebアクセス要求のフィルタリングをサポートしています。

SSL VPNゲートウェイは、次の手順を使用して、Webアクセス要求を転送するかどうかを決定します。

1. 要求を許可されたURLリストと照合します。
   - 要求がリスト内のURL項目と一致する場合、ゲートウェイは要求を転送します。
   - 要求がリスト内のどのURL項目とも一致しない場合、ゲートウェイは次の手順に進みます。
2. URI ACLの規則に対して要求を照合します。
   - 要求が許可規則に一致する場合、ゲートウェイは要求を転送します。
   - 要求が拒否規則と一致する場合、ゲートウェイは要求をドロップします。
   - 要求がURI ACLのどの規則とも一致しない場合、またはURI ACLが使用できない場合、ゲートウェイは次の手順に進みます。
3. 要求を拡張ACL内のルールと照合します。
   - 要求が許可規則に一致する場合、ゲートウェイは要求を転送します。
   - 要求が拒否規則と一致する場合、ゲートウェイは要求をドロップします。
   - 要求が拡張ACL内のどのルールとも一致しない場合、または拡張ACLが使用できない場合、ゲートウェイは要求をドロップします。

手順

1. システムビューに入ります。

   system-view
2. SSL VPNコンテキストビューを開始します。

   sslvpn context *context-name*
3. SSL VPNポリシーグループを作成し、SSL VPNポリシーグループビューを開始します。

   policy-group *group-name*
4. URLリストをポリシーグループに関連付けます。

   resources url-list *url-list-name*

   デフォルトでは、ポリシーグループに関連付けられたURLリストはありません。
5. (任意)WebアクセスフィルタリングのACLを指定します。
   - Webアクセスフィルタリング用の詳細ACLを指定します。

     filter web-access acl *advanced-acl-number*
   - Webアクセスフィルタリング用のURI ACLを指定します。

     filter web-access uri-acl *uri-acl-name*

   デフォルトでは、ユーザーはURLリストを通じて許可されたWebリソースにのみアクセスできます。

ファイルポリシーの構成

このタスクについて

ファイルポリシーを使用すると、SSL VPNゲートウェイは、要求元のWebアクセスユーザーに転送する前に、Webページファイルを書き換えることができます。

ファイルポリシーには、次の設定が含まれます。

- ファイルポリシーが適用されるファイルのパスを識別するURL。
- 1つ以上のリライトルール。

  リライトルールは、書き換えられる古いファイルの内容と、古い内容を置き換えるために使用される新しい内容を定義します。
- (任意)ファイルポリシーによって書き換えられた後にファイルが変更されるファイルタイプ。

手順

1. システムビューに入ります。

   system-view
2. SSL VPNコンテキストビューを開始します。

   sslvpn context *context-name*
3. ファイルポリシーを作成し、そのビューを入力します。

   file-policy *policy-name*

   デフォルトでは、ファイルポリシーは存在しません。
4. 書き直すファイルのURLを指定します。

   url *url*

   デフォルトでは、ファイルポリシーにファイルURLは指定されていません。
5. ファイルポリシーによって書き換えられた後にファイルが変更されるファイルタイプを指定します。

   content-type **{** css **|** html **|** javascript **|** other **}**

   デフォルトでは、ファイルポリシーはHTTP応答内のファイルを、HTTP応答のcontent-typeフィールドで指定されたファイルタイプに書き換えます。
6. リライトルールを作成し、そのビューを入力します。

   rewrite-rule *rule-name*
7. 書き換える古い内容を指定します。

   old-content *string*

   デフォルトでは、書き換えられる古いコンテンツは指定されていません。
8. 古いコンテンツを置き換えるために使用する新しいコンテンツを指定します。

   new-content *string*

   デフォルトでは、古いコンテンツを置き換えるために使用される新しいコンテンツは指定されていません。

TCPアクセスサービスの設定

リモートユーザーがTCPアクセスモードで内部リソースにアクセスできるようにするには、TCPアクセスリソースを設定し、そのリソースをSSL VPNポリシーグループに関連付ける必要があります。

TCPアクセスサービスタスクの概要

TCPアクセスサービスを設定するには、次のタスクを実行します。

1. ポート転送リストの設定
2. TCPアクセス用のSSL VPNポリシーグループの設定

ポート転送リストの設定

このタスクについて

ポート転送リストは、ポート転送項目のリストです。各ポート転送項目には、ポート転送インスタンスが含まれます。

ポート転送インスタンスは、内部サーバーでホストされているTCPサービス(Telnet、SSH、POP3など)をSSL VPNクライアントのローカルアドレスとポート番号にマッピングします。リモートユーザーは、ローカルアドレスとポート番号を使用してTCPサービスにアクセスできます。

ポート転送インスタンスは、ポート転送項目名とともにSSL VPN Webページに表示されます。ポート転送項目のリソースリンクを設定すると、ポート転送項目名がリンクとしてSSL VPN Webページに表示されます。リンクをクリックすると、リソースに直接アクセスできます。

手順

1. システムビューに入ります。

   system-view
2. SSL VPNコンテキストビューを開始します。

   sslvpn context *context-name*
3. ポート転送項目を作成し、そのビューを入力します。

   port-forward-item *item-name*
4. ポート転送項目のポート転送インスタンスを設定します。
   local-port *local-port-number* **local-name** *local-name* **remote-server** *remote-server* **remote-port** *remote-port-number* [**description** *text*]
5. SSL VPNコンテキストビューに戻ります。

   quit
6. ポート転送リストを作成し、そのビューを入力します。

   port-forward *port-forward-name*
7. ポート転送項目をポート転送リストに割り当てます。

   resources port-forward-item *item-name*

   デフォルトでは、ポート転送リストにポート転送項目は含まれていません。

TCPアクセス用のSSL VPNポリシーグループの設定

このタスクについて

TCPアクセス用のSSL VPNポリシーグループを設定するには、ポート転送リストをポリシーグループに関連付けます。認証サーバーがユーザーにポリシーグループの使用を許可すると、ユーザーはポリシーグループに関連付けられたポート転送リストによって提供されるTCPサービスにアクセスできます。

ポリシーグループでは、詳細ACLとURI ACLを指定して、ユーザーのTCPアクセス要求をフィルタリングできます。

拡張ACLは、宛先IPアドレスおよび宛先ポート番号によるTCPアクセス要求のフィルタリングをサポートします。URI ACLは、プロトコルタイプ、宛先アドレス、ドメイン名、ポート番号、およびURLによるTCPアクセス要求のフィルタリングをサポートします。

PCユーザーの場合、TCPアクセスフィルタリング用に設定されたACLは有効になりません。PCユーザーは、TCPポート転送リストを介して許可されたTCPリソースにのみアクセスできます。

モバイルクライアントユーザーの場合、SSL VPNゲートウェイは次の手順を使用して、TCPアクセス要求を転送するかどうかを決定します。

1. 要求を許可ポート転送リストと照合します。
   - 要求がリスト内のポート転送項目と一致する場合、ゲートウェイは要求を転送します。
   - 要求がリスト内のどのポート転送項目とも一致しない場合、ゲートウェイは次の手順に進みます。
2. URI ACLの規則に対して要求を照合します。
   - 要求が許可規則に一致する場合、ゲートウェイは要求を転送します。
   - 要求が拒否規則と一致する場合、ゲートウェイは要求をドロップします。
   - 要求がURI ACLのどの規則とも一致しない場合、またはURI ACLが使用できない場合、ゲートウェイは次の手順に進みます。
3. 要求を拡張ACLのルールと照合します。
   - 要求が許可規則に一致する場合、ゲートウェイは要求を転送します。
   - 要求が拒否規則と一致する場合、ゲートウェイは要求をドロップします。
   - 要求が拡張ACL内のどのルールとも一致しない場合、または拡張ACLが使用できない場合、ゲートウェイは要求をドロップします。

手順

1. システムビューに入ります。

   system-view
2. SSL VPNコンテキストビューを開始します。

   sslvpn context *context-name*
3. SSL VPNポリシーグループを作成し、SSL VPNポリシーグループビューを開始します。

   policy-group *group-name*
4. ポート転送リストをポリシーグループに関連付けます。

   resources port-forward *port-forward-name*

   デフォルトでは、ポート転送リストはポリシーグループに関連付けられていません。
5. (任意)TCPアクセスフィルタリングのACLを指定します。
   - TCPアクセスフィルタリングの詳細ACLを指定します。

     filter tcp-access acl *advanced-acl-number*
   - TCPアクセスフィルタリング用のURI ACLを指定します。

     filter tcp-access uri-acl *uri-acl-name*

   デフォルトでは、ユーザーはTCPポート転送リストを通じて認可されたTCPリソースだけにアクセスできます。

IPアクセスサービスの設定

リモートユーザーがIPアクセスモードで内部リソースにアクセスできるようにするには、IPアクセスリソースを設定し、そのリソースをSSL VPNポリシーグループに関連付ける必要があります。

IPアクセスサービスコンフィギュレーションの制約事項およびガイドライン

応答パケットがSSL VPNクライアントに正しく転送されるようにするには、内部サーバーからクライアントのVNICが存在するネットワークセグメントへのスタティックルートを設定します。

IPアクセスサービスタスクの概要

IPアクセスサービスを設定するには、次のタスクを実行します。

1. IPアクセス用のSSL VPN ACインターフェースの設定
2. IPアクセスユーザー用のアドレスプールの作成
3. SSL VPNコンテキストでのIPアクセスパラメーターの設定
4. IPアクセス用のSSL VPNポリシーグループの設定

IPアクセス用のSSL VPN ACインターフェースの設定

SSL VPN ACインターフェースの設定

1. システムビューに入ります。

   system-view
2. SSL VPN ACインターフェースを作成し、そのビューを入力します。

   interface sslvpn-ac *interface-number*
3. インターフェースのIPv4アドレスを設定します。

   ip address *ip-address* { *mask* | *mask-length* }

   デフォルトでは、ACインターフェースにIPv4アドレスは設定されていません。
4. (任意)インターフェースに予想される帯域幅を設定します。

   bandwidth *bandwidth-value*

   予想される帯域幅は、デフォルトで64 kbpsです。

   予想帯域幅は、上位層プロトコルでのみ計算に使用される情報パラメーターです。このコマンドを使用して、インターフェースの実際の帯域幅を調整することはできません。
5. (任意)インターフェースの説明を設定します。

   description *text*

   デフォルトのインターフェースの説明は、インターフェース名**Interface**です。次に例を示します。**SSLVPN-AC1000 Interface**。
6. (任意)インターフェースのMTUを設定します。

   mtu *size*

   デフォルトのMTUは1500バイトです。

7. インターフェースを始動します。

   undo shutdown

   デフォルトでは、SSL VPN ACインターフェースはアップしています。

SSL VPN ACインターフェースのデフォルト設定の復元

重要:

デフォルトのインターフェース設定を復元すると、進行中のネットワークサービスが中断される可能性があります。ライブネットワークで実行する場合は、この操作の影響を十分に認識していることを確認してください。

SSL VPN ACインターフェースのデフォルト設定を復元するには、次の手順を実行します。

1. システムビューに入ります。

   system-view

2. SSL VPN ACインターフェースビューを開始します。

   interface sslvpn-ac *interface-number*

3. SSL VPN ACインターフェースのデフォルト設定を復元します。

   default

   このコマンドは、コマンドの依存関係やシステムの制限などの理由で、一部のコマンドのデフォルト設定の復元に失敗する場合があります。インターフェースビューでこのコマンドを表示してこれらのコマンドを確認し、元に戻す形式を使用するか、コマンドリファレンスに従ってそれぞれのデフォルト設定を復元できます。それでも復元に失敗する場合は、エラーメッセージの指示に従って問題を解決してください。

IPアクセスユーザー用のアドレスプールの作成

このタスクについて

アドレスプールは、IPアクセスユーザーに割り当てることができるIPアドレスを定義します。

手順

1. システムビューに入ります。

   system-view

2. IPv4アドレスプールを作成します。

   sslvpn ip address-pool *pool-name start-ip-address end-ip-addr*

SSL VPNコンテキストでのIPアクセスパラメーターの設定

このタスクについて

IPアクセスユーザーにサービスを提供するには、SSL VPN ACインターフェース、アドレスプール、ルートリストなどのIPアクセスパラメーターをSSL VPNコンテキストで設定する必要があります。ユーザーがID認証に合格すると、SSL VPNコンテキストは、指定されたアドレスプールからユーザーのVNICにIPアドレスを割り当てます。ルートリストは、SSL VPNポリシーグループがユーザーにルートエントリを発行するために使用できます。

手順

1. システムビューに入ります。

   system-view
2. SSL VPNコンテキストビューを開始します。

   sslvpn context *context-name*
3. IPアクセス用のSSL VPN ACインターフェースを指定します。

   ip-tunnel interface sslvpn-ac *interface-number*

   デフォルトでは、SSL VPNコンテキストでIPアクセス用のSSL VPN ACインターフェースは指定されていません。
4. IPv4ルートリストを設定します。
   a. IPv4ルートリストを作成し、そのビューを入力します。

      ip-route-list *list-name*
   b. インクルードIPv4ルートをIPv4ルートリストに追加します。

      include *ip-address* { *mask* | *mask-length* }
   c. SSL VPNコンテキストビューに戻ります。

      quit
5. IPアクセス用のIPv4アドレスプールを指定します。

   ip-tunnel address-pool *pool-name* **mask** { *mask-length* | *mask* }

   デフォルトでは、IPアクセスにIPv4アドレスプールは指定されていません。
6. (任意)キープアライブインターバルを設定します。

   ip-tunnel keepalive *seconds*

   デフォルトでは、キープアライブインターバルは30秒です。
7. (任意)IPアクセス用のIPv4 DNSサーバーを指定します。

   ip-tunnel dns-server { **primary** | **secondary** } *ip-address*

   既定では、IPアクセスにIPv4 DNSサーバーは指定されていません。
8. (任意)IPアクセス用のWINSサーバーを指定します。

   ip-tunnel wins-server { **primary** | **secondary** } *ip-address*

   デフォルトでは、IPアクセス用のWINSサーバーは指定されていません。
9. (任意)Webログイン後のIPアクセスクライアントの自動起動をイネーブルにします。

   web-access ip-client auto-activate

   デフォルトでは、Webログイン後のIPアクセスクライアントの自動起動はディセーブルになっています。
10. (任意)Webページを介したIPアクセスユーザーへの、アクセス可能なリソースの自動プッシュをイネーブルにします。

    ip-tunnel web-resource auto-push

    デフォルトでは、Webページを介したIPアクセスユーザーへのアクセス可能なリソースの自動プッシュは無効になっています。
11. (任意)IPアクセスのアップストリームまたはダウンストリームトラフィックのレート制限を設定します。

    ip-tunnel rate-limit { **downstream** | **upstream** } { **kbps** | **pps** } *value*

    デフォルトでは、IPアクセスのアップストリームまたはダウンストリームトラフィックにレート制限は設定されていません。

IPアクセス用のSSL VPNポリシーグループの設定

このタスクについて

IPアクセス用のSSL VPNポリシーグループを設定するには、ポリシーグループ内のアクセス可能なIPリソースのルートを設定します。AAAサーバーまたはカスタム認証サーバーがユーザーにポリシーグループの使用を認可した後、SSL VPNゲートウェイはユーザーにルートを発行して、ユーザーがIPリソースにアクセスできるようにします。

次のいずれかの方法を使用して、ユーザーに発行するルートを設定できます。

- 手動でルートを設定します。
- ルートリストを指定します。
- すべてのトラフィックをSSL VPNゲートウェイに強制的に送信します。

  SSL VPNゲートウェイは、SSL VPNクライアントにデフォルトルートを発行します。デフォルトルートは、出力インターフェースとしてVNICを使用し、クライアント上のすべてのデフォルトルートの中で最も高いプライオリティを持ちます。ルーティングテーブルにない宛先へのパケットは、VNICを介してSSL VPNゲートウェイに送信されます。SSL VPNゲートウェイは、SSL VPNクライアントをリアルタイムで監視します。クライアントがデフォルトルートを削除したり、より高いプライオリティを持つデフォルトルートを追加したりすることはできません。

ポリシーグループでは、詳細ACLとURI ACLを指定して、ユーザーのIPアクセス要求をフィルタリングできます。

SSL VPNゲートウェイは、次の手順を使用して、IPアクセス要求を転送するかどうかを決定します。

1. URI ACLの規則に対して要求を照合します。
   - 要求が許可規則に一致する場合、ゲートウェイは要求を転送します。
   - 要求が拒否規則と一致する場合、ゲートウェイは要求をドロップします。
   - 要求がURI ACLのどの規則にも一致しない場合、またはURI ACLが使用できない場合、ゲートウェイはステップ2に進みます。
2. 要求を拡張ACLのルールと照合します。
   - 要求が許可規則に一致する場合、ゲートウェイは要求を転送します。
   - 要求が拒否規則と一致する場合、ゲートウェイは要求をドロップします。
   - 要求が拡張ACL内のどのルールとも一致しない場合、または拡張ACLが使用できない場合、ゲートウェイは要求をドロップします。

IPアクセスフィルタリングにURI ACLまたは拡張ACLが指定されていない場合、SSL VPNゲートウェイはデフォルトですべてのIPアクセスを許可します。

拡張ACLでは、次の基準を使用したIPアクセス要求のフィルタリングがサポートされています。

- 宛先IPアドレス。
- 宛先ポート番号。
- 送信元IPアドレス。
- 送信元ポート番号。
- プロトコルタイプ。
- パケットプライオリティ。
- フラグメント情報。
- TCPフラグ。

- ICMPメッセージタイプおよびメッセージコード。

URI ACLは、プロトコルタイプ、宛先アドレス、ドメイン名、ポート番号、およびURLによるIPアクセス要求のフィルタリングをサポートしています。

制限事項およびガイドライン

IPアクセスフィルタリングに指定されたURI ACL内の規則にHTTPまたはHTTPS設定が含まれている場合、その規則は有効になりません。

手順

1. システムビューに入ります。

   system-view
2. SSL VPNコンテキストビューを開始します。

   sslvpn context *context-name*
3. SSL VPNポリシーグループを作成し、SSL VPNポリシーグループビューを開始します。

   policy-group *group-name*
4. クライアントに発行されるIPv4ルートを指定します。
   ip-tunnel access-route { *ip-address* { *mask-length* | *mask* } | **force-all** | **ip-route-list** *list-name* }

   デフォルトでは、IPv4ルートは設定されていません。
5. IPアクセスフィルタリング用のACLを指定します。
   - IPアクセスフィルタリング用の詳細ACLを指定します。

     filter ip-tunnel acl *advanced-acl-number*
   - IPアクセスフィルタリング用のURI ACLを指定します。

     filter ip-tunnel uri-acl *uri-acl-name*

   デフォルトでは、SSL VPNゲートウェイはすべてのIPアクセス要求を許可します。
6. (任意)IPアクセス用のIPv4アドレスプールを指定します。

   ip-tunnel address-pool *pool-name* **mask** { *mask-length* | *mask* }

   デフォルトでは、SSL VPNポリシーグループのIPアクセスにIPv4アドレスプールは指定されていません。

   IPv4アドレスプールに使用可能な空きアドレスがない場合、またはIPv4アドレスプールが存在しない場合、IPアクセスユーザーへのアドレス割り当ては失敗し、ユーザーのアクセス要求は拒否されます。

   ポリシーグループにIPv4アドレスプールが指定されていない場合、SSL VPNゲートウェイは、SSL VPNコンテキストに指定されたIPv4アドレスプールからユーザーにIPv4アドレスを割り当てます。

モバイルクライアントのSSL VPNアクセスの設定

モバイルクライアントのSSL VPNアクセスタスクの概要

モバイルクライアントのSSL VPNアクセスを設定するには、次のタスクを実行します。

1. モバイルクライアント用のEMOサーバーの指定
2. (省略可能)モバイルクライアント用のメッセージサーバーの指定

モバイルクライアント用のEMOサーバーの指定

このタスクについて

EMOサーバーは、モバイルクライアントにサービスを提供します。モバイルクライアントにEMOサーバーを指定すると、SSL VPNゲートウェイはEMOサーバー情報をクライアントに発行します。クライアントは、EMOサーバーを介して使用可能なサービスリソースにアクセスできます。

手順

1. システムビューに入ります。
   system-view
2. SSL VPNコンテキストビューを開始します。
   sslvpn context *context-name*
3. モバイルクライアント用のEMOサーバーを指定します。
   emo-server address { *host-name* | *ipv4-address* } **port** *port-number*
   デフォルトでは、モバイルクライアントにEMOサーバーは指定されていません。

モバイルクライアント用のメッセージサーバーの指定

このタスクについて

メッセージサーバーは、モバイルクライアントにサービスを提供します。モバイルクライアントにメッセージサーバーを指定すると、SSL VPNゲートウェイはメッセージサーバー情報をクライアントに発行します。クライアントはメッセージサーバーにアクセスできます。

手順

1. システムビューに入ります。
   system-view
2. SSL VPNコンテキストビューを開始します。
   sslvpn context *context-name*
3. モバイルクライアント用のメッセージサーバーを指定します。
   message-server address { *host-name* | *ipv4-address* } **port** *port-number*
   デフォルトでは、モバイルクライアント用のメッセージサーバーは指定されていません。

ショートカットの設定

このタスクについて

内部サーバー上のリソースにすばやくアクセスできるようにするには、これらのリソースのショートカットを設定します。ショートカットは、SSL VPN Webページ上の保護されたリソースへのアクセスリンクを提供します。ユーザーは、SSL VPN Webページ上のショートカット名をクリックして、関連付けられたリソースにアクセスできます。

手順

1. システムビューに入ります。
   system-view
2. SSL VPNコンテキストビューを開始します。
   sslvpn context *context-name*

3. ショートカットを作成し、そのビューを入力します。
   shortcut *shortcut-name*-
   既定では、ショートカットはありません。
4. (省略可能)ショートカットの説明を設定します。
   description *text*
   デフォルトでは、ショートカットの説明は設定されていません。
5. ショートカットのリソースリンクを設定します。
   execution *script*
   デフォルトでは、ショートカットにリソースリンクは設定されていません。
6. SSL VPNコンテキストビューに戻ります。
   quit
7. ショートカットリストを作成し、そのビューを入力します。
   shortcut-list *list-name*
8. ショートカットをショートカットリストに割り当てます。
   resources shortcut *shortcut-name*
   既定では、ショートカットリストにショートカットは含まれていません。
9. SSL VPNコンテキストビューに戻ります。
   quit
10. SSL VPNポリシーグループビューを開始します。
    policy-group *group-name*
11. ショートカットリストをSSL VPNポリシーグループに割り当てます。
    resources shortcut-list *list-name*
    デフォルトでは、SSL VPNポリシーグループにショートカットリストは含まれていません。

リダイレクトリソースの構成

このタスクについて

デフォルトでは、ユーザーはSSL VPNゲートウェイにログインした後、SSL VPN Webページに入ります。内部サーバー上の指定されたWebリソースにすばやくアクセスできるようにするには、リソースをリダイレクトリソースとして設定します。ユーザーは、SSL VPN Webページに少し滞在した後、指定されたリダイレクトリソースを直接入力します。

手順

1. システムビューに入ります。
   system-view
2. SSL VPNコンテキストビューを開始します。
   sslvpn context *context-name*
3. SSL VPNポリシーグループビューを開始します。
   policy-group *group-name*
4. SSL VPNユーザーがログイン後にアクセスするWebリソースを設定します。
   redirect-resource { **shortcut** | **url-item** } *resource-name*

デフォルトでは、SSL VPNゲートウェイにログインした後、ユーザーはSSL VPN Webページに直接入り、リダイレクションは実行されません。

HTTPリダイレクションの設定

このタスクについて

SSL VPNゲートウェイは、HTTPSを介してユーザーと通信します。HTTPがSSL VPNゲートウェイにアクセスできるようにするには、HTTPリダイレクションを設定する必要があります。

HTTPリダイレクションを使用すると、SSL VPNゲートウェイで次の操作を実行できます。

1. HTTPポートをリッスンします。
2. ポート番号を持つHTTP要求を、HTTPSで使用されるポートにリダイレクトします。
3. リダイレクションパケットをクライアントに送信します。

手順

1. システムビューに入ります。

   system-view
2. SSL VPNゲートウェイビューを開始します。

   sslvpn gateway *gateway-name*
3. HTTPリダイレクションをイネーブルにします。

   http-redirect [**port** *port-number*]

   デフォルトでは、HTTPリダイレクションはディセーブルになっています。SSL VPNゲートウェイはHTTPトラフィックを処理しません。

SSL VPNコンテキストのデフォルトポリシーグループの設定

このタスクについて

ユーザーのログイン後に、AAAサーバーまたはカスタム認証サーバーがポリシーグループをユーザーに認可しない場合、SSL VPNゲートウェイはデフォルトポリシーグループをユーザーに認可します。デフォルトポリシーグループが設定されていない場合、SSL VPNゲートウェイはユーザーからのすべてのアクセス要求を拒否します。

手順

1. システムビューに入ります。

   system-view
2. SSL VPNコンテキストビューを開始します。

   sslvpn context *context-name*
3. SSL VPNポリシーグループを作成し、SSL VPNポリシーグループビューを開始します。

   policy-group *group-name*
4. ポリシーグループでアクセス可能なリソースを設定します。
   - Webアクセスリソースを構成します。

resources url-list *url-list-name*

デフォルトでは、ポリシーグループにURLリストは指定されていません。

- TCPアクセスリソースを設定します。

  resources port-forward *port-forward-name*

  デフォルトでは、ポリシーグループにポート転送リストは指定されていません。

- IPv4アクセスリソースを構成します。

  ip-tunnel access-route { *ip-address* { *mask-length* | *mask* } | **force-all** | **ip-route-list** *list-name* }

  デフォルトでは、ポリシーグループにIPv4ルートエントリは設定されていません。

5. (任意)WebアクセスフィルタリングのACLを指定します。
   - Webアクセスフィルタリング用の詳細ACLを指定します。

     filter web-access acl *advanced-acl-number*

   - Webアクセスフィルタリング用のURI ACLを指定します。

     filter web-access uri-acl *uri-acl-name*

   デフォルトでは、ユーザーはURLリストを通じて許可されたWebリソースにのみアクセスできます。
6. (任意)TCPアクセスフィルタリングのACLを指定します。
   - TCPアクセスフィルタリングの詳細ACLを指定します。

     filter tcp-access acl *advanced-acl-number*

   - TCPアクセスフィルタリング用のURI ACLを指定します。

     filter tcp-access uri-acl *uri-acl-name*

   デフォルトでは、ユーザーはTCPポート転送リストを通じて認可されたTCPリソースだけにアクセスできます。
7. (任意)IPアクセスフィルタリングのACLを指定します。
   - IPアクセスフィルタリング用の詳細ACLを指定します。

     filter ip-tunnel acl *advanced-acl-number*

   - IPアクセスフィルタリング用のURI ACLを指定します。

     filter ip-tunnel uri-acl *uri-acl-name*

   デフォルトでは、SSL VPNゲートウェイはすべてのIPアクセス要求を許可します。
8. SSL VPNコンテキストビューに戻ります。

   quit
9. ポリシーグループをSSL VPNコンテキストのデフォルトポリシーグループとして指定します。

   default-policy-group *group-name*

   デフォルトでは、SSL VPNコンテキストにデフォルトポリシーグループは指定されていません。

VRF-aware SSL VPNの設定

SSL VPNコンテキストとVPNインスタンスの関連付け

このタスクについて

異なるSSL VPNコンテキストをSSL VPNゲートウェイ上の異なるVPNインスタンスに関連付けることがで

きます。SSL VPNコンテキスト内のユーザーは、SSL VPNコンテキストに関連付けられたVPNインスタンス内のリソースにだけアクセスできます。VRF認識SSL VPNコンテキストでは、サーバードレスのオーバーラップも許可されます。

前提条件

この機能を設定する前に、次の作業を完了してください。

- VPNインスタンスを作成します。
- 内部サーバーに接続されているSSL VPNゲートウェイのインターフェースをVPNインスタンスに関連付けます。
- (IPアクセスの場合は必須)ip-tunnel interfaceコマンドで指定したSSL VPN ACインターフェースをVPNインスタンスに関連付けます。

VPNインスタンスの詳細については、『MPLS Configuration Guide』の「MPLS L3VPN configuration」を参照してください。

手順

1. システムビューに入ります。

   system-view
2. SSL VPNコンテキストビューを開始します。

   sslvpn context *context-name*
3. SSL VPNコンテキストをVPNインスタンスに関連付けます。

   vpn-instance *vpn-instance-name*

   デフォルトでは、SSL VPNコンテキストはパブリックネットワークに関連付けられています。

SSL VPNゲートウェイのVPNインスタンスの指定

このタスクについて

SSL VPNゲートウェイのVPNインスタンスを指定すると、指定したVPN内のユーザーだけがSSL VPNゲートウェイにアクセスできます。VRF対応SSL VPNゲートウェイは、内部サーバーリソースがパブリックネットワークまたは他のVPNに漏れるのを防ぎます。

前提条件

この機能を設定する前に、次の作業を完了してください。

- VPNインスタンスを作成します。
- VPNインスタンスを、ユーザーに接続されているSSL VPNゲートウェイのインターフェースに関連付けます。
- SSL VPN ACインターフェースにバインドします。

手順

1. システムビューに入ります。

   system-view
2. SSL VPNゲートウェイビューを開始します。

   sslvpn gateway *gateway-name*
3. ゲートウェイのVPNインスタンスを指定します。

   vpn-instance *vpn-instance-name*

デフォルトでは、SSL VPNゲートウェイはパブリックネットワークに属しています。

オンラインSSL VPNユーザー制御の設定

このタスクについて

強制ログアウト機能、各アカウントの最大同時ログイン数、セッションごとに許可される最大接続数など、SSL VPNユーザーログイン制御機能を設定するには、次の作業を実行します。

手順

1. システムビューに入ります。

   system-view
2. SSL VPNコンテキストビューを開始します。

   sslvpn context *context-name*
3. オンラインユーザーにログアウトを強制します。

   force-logout [**all** | **session** *session-id* | **user** *user-name*]
4. 各アカウントの最大同時ログイン数を設定します。

   max-onlines *number*

   デフォルトでは、各アカウントの同時ログインの最大数は32です。
5. 強制ログアウト機能をイネーブルにします。

   force-logout max-onlines enable

   デフォルトでは、強制ログアウト機能は無効になっています。アカウントを使用したログイン数が最大に達した場合、ユーザーはログインできません。

   ログインが試行されたが、そのアカウントを使用したログインが最大数に達した場合、この機能は、新しいログインを許可するために最も長いアイドル時間でユーザーをログアウトします。
6. セッションごとに許可される最大接続数を設定します。

   session-connections *number*

   デフォルトでは、セッションごとに最大64の接続が許可されます。

   セッション内の接続数が最大数に達した場合、そのセッションに対する新しい接続要求は503 Service Unavailableメッセージとともに拒否されます。

SSL VPNセッションレート制限の設定

このタスクについて

SSL VPNセッションのアップストリームトラフィックとダウンストリームトラフィックのレート制限をそれぞれ設定するには、次の作業を実行します。SSL VPNセッションのアップストリームトラフィックまたはダウンストリームトラフィックがレート制限を超えると、後続のアップストリームトラフィックまたはダウンストリームトラフィックは廃棄されます。

手順

1. システムビューに入ります。

   system-view
2. SSL VPNコンテキストビューを開始します。

sslvpn context *context-name*

3. SSL VPNセッションのアップストリームまたはダウンストリームトラフィックのレート制限を設定します。

   rate-limit { **downstream** | **upstream** } *value*

   デフォルトでは、SSL VPNセッションのアップストリームまたはダウンストリームトラフィックにレート制限は設定されていません。

SSL VPNクラッキング防止の設定

このタスクについて

この機能は、同じIPアドレスからのログイン試行回数を制限することで、ユーザーログイン情報のブルートフォースクラッキングのリスクを軽減します。

同じIPアドレスの連続ログイン失敗回数が指定された回数に達した場合、IPアドレスは指定された期間凍結されます。凍結期間中、IPアドレスはSSL VPNコンテキストへのログインを禁止されます。凍結期間が終了すると、凍結されたIPアドレスは自動的に凍結解除されます。凍結されたIPアドレスをただちに凍結解除するには、prevent-cracking unfreeze-ipコマンドを実行します。

手順

1. システムビューに入ります。

   system-view

2. SSL VPNコンテキストビューを開始します。

   sslvpn context *context-name*

3. クラック防止のためにIPアドレスのフリーズをイネーブルにします。

   prevent-cracking freeze-ip enable

   デフォルトでは、クラッキング防止のためのIPアドレスフリーズはディセーブルになっています。

4. (任意)IPアドレスで許容される連続ログイン失敗の最大回数、およびクラッキング防止のためにIPアドレスをフリーズする期間を指定します。

   prevent-cracking freeze-ip login-failures *login-failures* **freeze-time** *freeze-time*

   デフォルトでは、IPアドレスに許可される連続ログイン失敗の最大数は64で、IPアドレスをフリーズする時間は30秒です。

5. クラック防止のためのコード検証を有効にします。

   prevent-cracking verify-code enable

   デフォルトでは、クラッキング防止のためのコード検証は無効になっています。

6. (任意)クラッキングを防ぐためにコード検証を実行する前に、IPアドレスに許可される連続ログイン失敗の最大回数を指定します。

   prevent-cracking verify-code login-failures *login-failures*

   デフォルトでは、コード検証を実行する前に、IPアドレスに対して最大5回の連続したログイン失敗が許可されます。

7. (任意)フリーズされたIPアドレスのフリーズを解除します。

   prevent-cracking unfreeze-ip { **all** | **ipv4** *ip-address* }

SSL VPN SSOログインの設定

SSL VPN SSOログインの設定について

SSOを使用すると、ユーザーは1セットのログインクレデンシャル(ユーザー名やパスワードなど)を使用して、複数の信頼されたシステムにアクセスできます。SSOを使用すると、SSL VPN Webアクセスユーザーは、内部サーバーのログインクレデンシャルを入力しなくても、内部サーバーにアクセスできます。デバイスでは、SSOログインに次の方式がサポートされています。

- **自動ビルド方式(ログイン要求を自動的にビルド)**

  パケットキャプチャツールを使用して内部サーバーログイン要求を取得し、ログイン要求に基づいてSSOログイン設定を構成して、内部サーバーへのログイン要求を自動的に構築します。SSOログイン設定には、HTTP要求方式、ログイン要求のエンコード方式、ログインパラメーター、およびログインデータ暗号化ファイルが含まれます。

- **基本認証方式**

  基本認証は、単純なHTTP認証スキームで、Webクライアントがサーバーにアクセスするためにユーザー名とパスワードを入力する必要があります。サーバーは、ユーザー名とパスワードに基づいてクライアントを認証します。

  基本認証方式でSSOを実装するには、SSL VPNゲートウェイがWebクライアントとして動作し、ユーザー名とパスワードを自動的に入力してHTTP基本認証を実行します。入力するユーザー名とパスワードは、SSL VPNユーザー名とパスワードまたはカスタムユーザー名とパスワードのいずれかです。

  基本認証SSO方式は、基本認証をサポートする内部サーバーへのログインにだけ適用できます。

制限事項およびガイドライン

自動ビルドSSO方式の場合、次の要件を満たす必要があります。

- SSOログインは、SSL VPN Webアクセスユーザーだけが使用できます。
- ユーザーグループ名がSSOログインパラメーターとして指定されている場合は、リモートユーザーのみがサポートされます。
- SSOログインは、SSL VPN Webインターフェース上のURLリンクをクリックしてリソースにアクセスする場合にだけ使用できます。ブラウザのアドレスバーまたはURL入力ボックスにURLを入力してリソースにアクセスする場合、SSOは機能しません。
- SSOログインは、グラフィック検証コードを必要とするWebリソースでは使用できません。
- SSOログインは、Two-Factor認証またはスクリプト呼び出しを必要とするWebリソースでは使用できません。

自動ビルド方式でのSSOログインの設定

1. システムビューに入ります。

   シsystem-view

2. SSL VPNコンテキストビューを開始します。

   sslvpn context *context-name*

3. URLアイテムを作成し、そのビューを入力します。

   url-item *name*

4. URL項目にリソースURLを指定します。

   url *url*

デフォルトでは、URL項目にリソースURLは指定されていません。

リソースURLでプロトコルタイプを指定しない場合、デフォルトのプロトコル(HTTP)が使用されます。

5. WebアクセスSOOを有効にし、自動構築方法を指定します。

   sso method auto-build

   デフォルトでは、WebアクセスSSOログインは無効になっています。

6. SSOログイン要求を送信するためのHTTP要求方式を指定します。

   sso auto-build request-method **{** get **|** post **}**

   デフォルトでは、GET要求メソッドがSSOログイン要求の送信に使用されます。

7. SSOログイン要求のエンコード方式を指定します。

   sso auto-build code **{** gb18030 **|** utf-8 **}**

   デフォルトでは、SSOログイン要求にはUTF-8エンコードが使用されます。

8. SSOログイン要求を自動的に構築するためのログインパラメーターを設定します。

   sso auto-build login-parameter { **cert-fingerprint** | **cert-serial** | **cert-title** | **custom-password** | **custom-username** | **login-name** | **login-password** | **mobile-num** | **user-group** } **name** *parameter-name* [**encrypt**]

   デフォルトでは、SSOログイン要求の自動構築用のログインパラメーターは設定されていません。

9. SSOログイン要求を自動的に構築するためのカスタムログインパラメーターを設定します。

   sso auto-build custom-login-parameter name *parameter-name* **value** *value* [**encrypt**]

   デフォルトでは、SSOログイン要求の自動構築用のカスタムパラメーターは設定されていません。

10. SSOログイン要求のパラメーターの値を暗号化する暗号化ファイルを指定します。

    sso auto-build encrypt-file *filename*

    デフォルトでは、暗号化ファイルは指定されていません。

基本認証によるSSOログインの構成

1. システムビューに入ります。

   system-view

2. SSL VPNコンテキストビューを開始します。

   sslvpn context *context-name*

3. URLアイテムを作成し、そのビューを入力します。

   url-item *name*

4. URL項目にリソースURLを指定します。

   url *url*

   デフォルトでは、URL項目にリソースURLは指定されていません。

   リソースURLでプロトコルタイプを指定しない場合、デフォルトのプロトコル(HTTP)が使用されます。

5. WebアクセスSSOを有効にし、SSO方式を基本認証として指定します。

sso method basic

デフォルトでは、WebアクセスSSOログインは無効になっています。

6. (任意)基本認証によるSSOログインにカスタムユーザー名とパスワードを使用することをイネーブルにします。

   sso basic custom-username-password enable

   デフォルトでは、SSL VPNログインのユーザー名とパスワードが、基本認証によるSSOログインに使用されます。

拒否されたSSL VPNクライアントタイプの設定

このタスクについて

ユーザーが特定のタイプのクライアントソフトウェアを使用してSSL VPNゲートウェイにログインすることを拒否するには、次の作業を実行して、拒否するSSL VPNクライアントソフトウェアのタイプを指定します。

制限事項およびガイドライン

ブラウザが拒否されると、既存のユーザーと新しいユーザーは、ブラウザを使用してSSL VPNゲートウェイにアクセスできなくなります。ブラウザがSSL VPNアクセスの権限を回復した後、ユーザーはログインページを更新してログインする必要があります。他のクライアントタイプの拒否は、新しいユーザーに対してのみ有効です。既存のユーザーには影響しません。

手順

1. システムビューに入ります。

   system-view

2. SSL VPNコンテキストビューを開始します。

   sslvpn context *context-name*

3. SSL VPNへのアクセスを拒否するクライアントタイプを設定します。

   access-deny-client **{** browser **|** mobile-inode **|** pc-inode **} ***

   デフォルトでは、SSL VPNへのアクセスが拒否されるクライアントタイプはありません。

SSL VPN Webページのカスタマイズ

制限事項およびガイドライン

ユーザー定義のWebページテンプレートがSSL VPNコンテキストで指定されている場合、他のすべてのWebページカスタマイゼーション設定はSSL VPNコンテキストに対して無効になります。

SSL VPN Webページ要素のカスタマイズ

このタスクについて

SSL VPN Webページでは、次の要素をカスタマイズできます。

- ログインメッセージ。
- パスワード入力ボックスの表示。
- タイトル。

- ロゴ。
- SSL VPNゲートウェイログインページおよびリソースページの通知メッセージ。
- ユーザーがSSL VPNリソースページでダウンロードするファイル。
- パスワードの複雑さの説明。
- サーバー応答メッセージの書き換え。

手順

1. システムビューに入ります。
   system-view
2. SSL VPNコンテキストビューを開始します。
   sslvpn context *context-name*
3. ログインメッセージを設定します。
   login-message { **chinese** *chinese-message* | **english** *english-message* }
   デフォルトでは、ログインメッセージはWelcome to SSL VPNです。
4. SSL VPN Webログインページのパスワード入力ボックスを非表示にします。
   password-box hide
   デフォルトでは、SSL VPN Webログインページにパスワード入力ボックスが表示されます。
5. タイトルを設定します。
   title { **chinese** *chinese-title* | **english** *english-title* }
   デフォルトでは、タイトルはSSL VPNです。
6. ロゴを指定してください
   logo { **file** *file-name* | **none** }
   デフォルトでは、H3Cロゴが表示されます。
7. SSL VPNゲートウェイのログインページまたはリソースページに表示される通知メッセージを設定します。
   notify-message { **login-page** | **resource-page** } { **chinese**
   ***chinese-message* |** english ***english-message* }**
   デフォルトでは、通知メッセージは設定されていません。
8. SSL VPNゲートウェイリソースページで、ユーザーがダウンロードするファイルを指定します。
   resources-file { **chinese** *chinese-filename* | **english**
   english-filename }
   デフォルトでは、ユーザーがダウンロードできるファイルは提供されていません。
9. SSL VPNパスワード変更ページに表示されるパスワードの複雑度メッセージを設定します。
   password-complexity-message { **chinese** *chinese-message* | **english**
   english-message }
   デフォルトでは、パスワードの複雑度メッセージは設定されていません。
10. サーバー応答メッセージを書き換えます。
    rewrite server-response-message *server-response-message* { **chinese**
    chinese-message | **english** *english-message* }
    デフォルトでは、サーバー応答メッセージは書き換えられません。

SSL VPN Webページテンプレートの指定

このタスクについて

このタスクでは、SSL VPN Webページテンプレートを指定して、SSL VPN Webページをカスタマイズできます。SSL VPN Webページテンプレートは、SSL VPNゲートウェイログインページおよびリソースページのスタイルを定義します。

Webページテンプレートは、システムビューおよびSSL VPNコンテキストビューで指定できます。

- システムビューで設定されたWebページテンプレートは、グローバルSSL VPN Webページテンプレートで、すべてのSSL VPNコンテキストに適用できます。
- SSL VPNコンテキストビューで設定されたWebページテンプレートは、現在のSSL VPNコンテキストにだけ適用できます。

前提条件

ユーザー定義のWebページテンプレートを、Webページからデバイスのファイルシステムにアップロードします。

SSL VPN Webページカスタマイゼーションの制約事項およびガイドライン

SSL VPNコンテキストビューで指定されたSSL VPN Webページテンプレートは、システムビューのテンプレートよりも優先されます。

システムビューでのSSL VPN Webページテンプレートの指定

1. システムビューに入ります。

   system-view
2. グローバルSSL VPN Webページテンプレートを指定します。

   sslvpn webpage-customize *template-name*

   デフォルトでは、グローバルSSL VPN Webページテンプレートは指定されていません。SSL VPNは、システムのデフォルトSSL VPN Webページを使用します。

SSL VPNコンテキストでのSSL VPN Webページテンプレートの指定

1. システムビューに入ります。

   system-view
2. SSL VPNコンテキストビューを開始します。

   sslvpn context *context-name*
3. SSL VPN Webページテンプレートを指定します。

   webpage-customize *template-name*

   デフォルトでは、SSL VPNコンテキストにSSL VPN Webページテンプレートは指定されていません。SSL VPNコンテキストは、グローバルSSL VPN Webページテンプレートを使用します。

SSL VPNロギングのイネーブル化

このタスクについて

SSL VPNロギングによって生成されたログは、デバイスのInformation Centerに送信されます。ログを正しく出力するには、デバイスにInformation Centerを設定する必要もあります。Information Centerの詳細については、『Network Management and Monitoring Configuration Guide』を参照してください。

手順

1. システムビューに入ります。
   system-view
2. SSL VPNグローバルロギング機能をイネーブルにします。
   sslvpn log enable
   デフォルトでは、SSL VPNグローバルロギング機能はディセーブルになっています。
3. SSL VPNコンテキストビューを開始します。
   sslvpn context *context-name*
4. ユーザーログインおよびログオフイベントのロギングを使用可能にします。
   log user-login enable
   デフォルトでは、ユーザーログインおよびログオフイベントのロギングは使用不可になっています。
5. ユーザーのリソースアクセスのロギングを使用可能にします。
   log resource-access enable **[** brief **|** filtering **] ***
   デフォルトでは、リソースアクセスロギングは使用不可になっています。
6. IPアクセス接続クローズイベントのロギングをイネーブルにします。
   ip-tunnel log connection-close
   デフォルトでは、IPアクセス接続クローズイベントのロギングはディセーブルになっています。
7. IPアクセスパケットドロップイベントのロギングをイネーブルにします。
   ip-tunnel log packet-drop
   デフォルトでは、IPアクセスパケットドロップイベントのロギングはディセーブルです。
8. IPアクセスクライアントのVNICのIPアドレス割り当ておよびリリースのロギングをイネーブルにします。
   ip-tunnel log address-alloc-release
   デフォルトでは、IPアクセスクライアントのVNICに対するIPアドレスの割り当ておよび解放のロギングはディセーブルになっています。

SSL VPNの表示およびメンテナンスコマンド

任意のビューでdisplayコマンドを実行し、ユーザービューでコマンドをリセットします。

タスク	**コマンド**
SSL VPN ACインターフェース情報を表示します。	**display interface sslvpn-ac** [*interface-number*] [**brief** [**description** | **down**]]
SSL VPNコンテキスト情報を表示します。	**display sslvpn context** [**brief** | **name** *context-name*]
SSL VPNゲートウェイ情報を表示します。	**display sslvpn gateway** [**brief** | **name** *gateway-name*]
IPアクセスユーザーのパケット統計情報を表示します。	**display sslvpn ip-tunnel statistics** [**context** *context-name*] [**user** *user-name*]

SSL VPNポリシーグループ情報を表示します。	**display sslvpn policy-group** *group-name* [**context** *context-name*]
TCPポート転送接続情報を表示します。	**display sslvpn port-forward connection** [**context** *context-name*] In IRF mode: **display sslvpn port-forward connection** [**context** *context-name*] [**slot** *slot-number*]
クラッキング防止のためにフリーズされたIPアドレスに関する情報を表示します。	**display sslvpn prevent-cracking frozen-ip** { **statistics** | **table** } [**context** *context-name*]
SSL VPNセッション情報を表示します。	**display sslvpn session** [**context** *context-name*] [**user** *user-name* | **verbose**]
SSL VPN Webページテンプレート情報を表示します。	**display sslvpn webpage-customize** template
SSL VPN ACインターフェース統計情報をクリアします。	**reset counters interface** [**sslvpn-ac** [*interface-number*]]
IPアクセスユーザーのパケット統計情報をクリアします。	**reset sslvpn ip-tunnel statistics** [**context** *context-name* [**session** *session-id*]]

SSL VPNの設定例

例:自己署名証明書を使用したWebアクセスの構成

ネットワーク構成

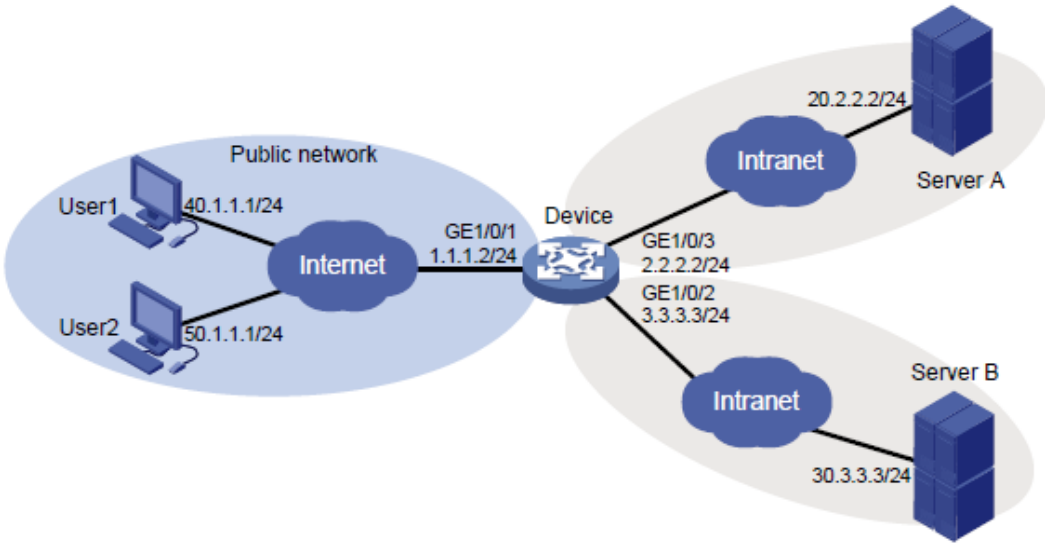
図11に示すように、デバイスはパブリックネットワークとプライベートネットワークを接続するSSL VPNゲートウェイとして機能します。サーバーAとサーバーBは内部Webサーバーです。サーバーAはポート80経由でHTTPを使用します。サーバーBはポート443経由でHTTPSを使用します。

デバイスは、自己署名SSLサーバー証明書を使用します。

デバイスでSSL VPN Webアクセスを設定して、ユーザー1がサーバーAだけにアクセスし、ユーザー2がサーバーBだけにアクセスできるようにします。

ユーザーのローカル認証および認可を実行するように、デバイスを設定します。

図11 ネットワークダイアグラム



手順

1. デバイス上のインターフェースのIPアドレスを設定します(詳細は省略)。
2. デバイスとユーザー、デバイスとサーバーA、およびデバイスとサーバーBが相互に到達できることを確認します(詳細は省略)。
3. SSL VPNゲートウェイを設定します。

   #SSL VPNゲートウェイgwのIPアドレスを1.1.1.2に、ポート番号を4430に設定します。

   <Device> system-view

   [Device] sslvpn gateway gw

   [Device-sslvpn-gateway-gw] ip address 1.1.1.2 port 4430

   #SSL VPNゲートウェイをイネーブルにします。

   [Device-sslvpn-gateway-gw] service enable

   [Device-sslvpn-gateway-gw] quit
4. SSL VPNコンテキストを設定します。

   #SSL VPNコンテキストctxweb1を作成してから、ゲートウェイgwとドメインdomainweb1を指定します。と入力します。

   [Device] sslvpn context ctxweb1

   [Device-sslvpn-context-ctxweb1] gateway gw domain domainweb1

   #urlitemという名前のURL項目を作成し、そのURL項目にリソースURLを指定します。

   [Device-sslvpn-context-ctxweb1] url-item urlitem

   [Device-sslvpn-context-ctxweb1-url-item-urlitem] url http://20.2.2.2

   [Device-sslvpn-context-ctxweb1-url-item-urlitem] quit

   #SSL VPNコンテキストctxweb1にurllistという名前のURLリストを作成します。

   [Device-sslvpn-context-ctxweb1] url-list urllist

#URLリストの見出しをwebに設定します。
[Device-sslvpn-context-ctxweb1-url-list-urllist] heading web
#URLアイテムurlitemをURLリストurllistに割り当てます。
[Device-sslvpn-context-ctxweb1-url-list-urllist] resources url-item urlitem
[Device-sslvpn-context-ctxweb1-url-list-urllist] quit
#SSL VPNコンテキストresourcegrp1用にctxweb1という名前のSSL VPNポリシーグループを作成し、Webアクセス用のポリシーグループにURLリストurllistを追加します。
[Device-sslvpn-context-ctxweb1] policy-group resourcegrp1
[Device-sslvpn-context-ctxweb1-policy-group-resourcegrp1] resources url-list urllist
[Device-sslvpn-context-ctxweb1-policy-group-resourcegrp1] quit
#SSL VPNコンテキストctxweb1をイネーブルにします。
[Device-sslvpn-context-ctxweb1] service enable
[Device-sslvpn-context-ctxweb1] quit
#SSL VPNコンテキストctxweb2を作成してから、ゲートウェイgwとドメインdomainweb2を指定します。と入力します。
[Device] sslvpn context ctxweb2
[Device-sslvpn-context-ctxweb2] gateway gw domain domainweb2
#urlitemという名前のURL項目を作成し、そのURL項目にリソースURLを指定します。
[Device-sslvpn-context-ctxweb1] url-item urlitem
[Device-sslvpn-context-ctxweb1-url-item-urlitem] url http://30.3.3.3
[Device-sslvpn-context-ctxweb1-url-item-urlitem] quit
#SSL VPNコンテキストctxweb2にurllistという名前のURLリストを作成します。
[Device-sslvpn-context-ctxweb2] url-list urllist
#URLリストの見出しをwebに設定します。
[Device-sslvpn-context-ctxweb2-url-list-urllist] heading web
#URLアイテムurlitemをURLリストurllistに割り当てます。
[Device-sslvpn-context-ctxweb1-url-list-urllist] resources url-item urlitem
[Device-sslvpn-context-ctxweb1-url-list-urllist] quit
#SSL VPNコンテキストresourcegrp2用にctxweb2という名前のSSL VPNポリシーグループを作成し、Webアクセス用のポリシーグループにURLリストurllistを追加します。
[Device-sslvpn-context-ctxweb2] policy-group resourcegrp2
[Device-sslvpn-context-ctxweb2-policy-group-resourcegrp2] resources url-list urllist
[Device-sslvpn-context-ctxweb2-policy-group-resourcegrp2] quit
#SSL VPNコンテキストctxweb2をイネーブルにします。
[Device-sslvpn-context-ctxweb2] service enable

[Device-sslvpn-context-ctxweb2] quit

5. SSL VPNユーザーを設定します。

#user 1のローカルユーザーカウントを作成します。ユーザー名を**sslvpnuser1**、パスワードを**123456 TESTplat&!**、サービスタイプを**sslvpn**、ユーザーロールを**network-operator**に設定します。ユーザーにポリシーグループ**resourcegrp1**の使用を許可します。

[Device] local-user sslvpnuser1 class network

[Device-luser-network-sslvpnuser1] password simple 123456TESTplat&!

[Device-luser-network-sslvpnuser1] service-type sslvpn

[Device-luser-network-sslvpnuser1] authorization-attribute user-role network-operator

[Device-luser-network-sslvpnuser1] authorization-attribute sslvpn-policy-group resourcegrp1

[Device-luser-network-sslvpnuser1] quit

#user 2のローカルユーザーカウントを作成します。ユーザー名を**sslvpnuser2**に、パスワードを**123456 TESTplat&!**に、サービスタイプを**sslvpn**に、ユーザーロールを**network-operator**に設定します。ユーザーにポリシーグループ**resourcegrp2**の使用を許可します。

[Device] local-user sslvpnuser2 class network

[Device-luser-network-sslvpnuser2] password simple 123456TESTplat&!

[Device-luser-network-sslvpnuser2] service-type sslvpn

[Device-luser-network-sslvpnuser2] authorization-attribute user-role network-operator

[Device-luser-network-sslvpnuser2] authorization-attribute sslvpn-policy-group resourcegrp2

[Device-luser-network-sslvpnuser2] quit

設定の確認

#デバイスでSSL VPNゲートウェイgwが起動していることを確認します。

[Device] display sslvpn gateway

Gateway name: gw

Operation state: Up

IP: 1.1.1.2 Port: 4430

Front VPN instance: Not configured

#SSL VPNコンテキストctxweb1およびctxweb2がデバイスでアップしていることを確認します。

[Device] display sslvpn context

Context name: ctxweb1

Operation state: Up

AAA domain: Not specified

Certificate authentication: Disabled

Password authentication: Enabled

Authentication use: All
Code verification: Disabled
Default policy group: Not configured
Associated SSL VPN gateway: gw
Domain name: domainweb1
Maximum users allowed: 1048575
VPN instance: Not configured
Idle timeout: 30 min
Password changing: Enabled
Denied client types: Browsers

Context name: ctxweb2
Operation state: Up
AAA domain: Not specified
Certificate authentication: Disabled
Password authentication: Enabled
Authentication use: All
Code verification: Disabled
Default policy group: Not configured
Associated SSL VPN gateway: gw
Domain name: domainweb2
Maximum users allowed: 1048575
VPN instance: Not configured
Idle timeout: 30 min
Password changing: Enabled
Denied client types: Browsers

#ユーザー1のパソコンで、ブラウザのアドレスバーにhttps://1.1.1.2:4430/と入力して、ドメイン一覧ページを開きます。

注:

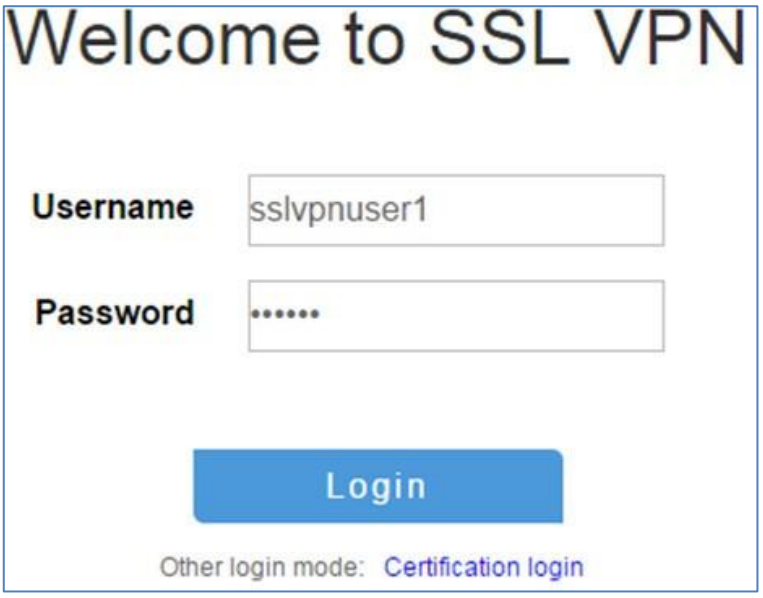
SSL VPNゲートウェイは自己署名のSSLサーバー証明書を使用するため、ゲートウェイにアクセスしようとすると、ブラウザに証明書が信頼されていないというエラーが表示されます。ゲートウェイへのアクセスを続行するには、を選択します。

図12ドメインリストページ

domainweb1を選択して、ログインページにアクセスします。

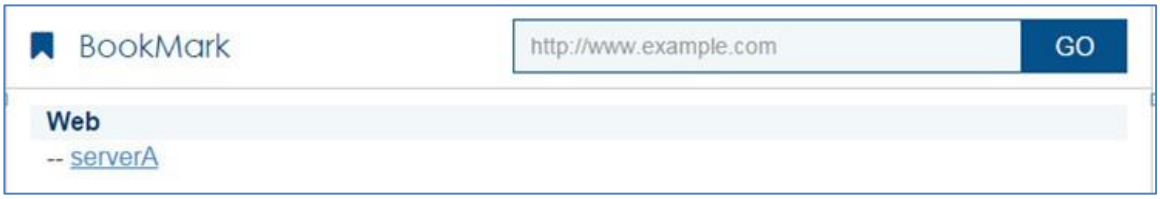
#ログインページで、ユーザー名**sslvpnuser1**とパスワード**123456 TESTplat&!**を入力し、**Login**をクリックします。

図13 ログインページ



#SSL VPNホームページが開き、ユーザーがアクセスできるWebリソースが**BookMark**領域に表示されます。この例では、図14に示すように**serverA**が表示されます。**serverA**リンクをクリックして、サーバーA上のWebリソースにアクセスします。

図14 SSL VPNゲートウェイのホームページ



ユーザー2のパソコンで、ブラウザのアドレスバーに**https://1.1.1.2:4430/**と入力して、ドメイン一覧ページを開きます。

図15 ドメインリストページ

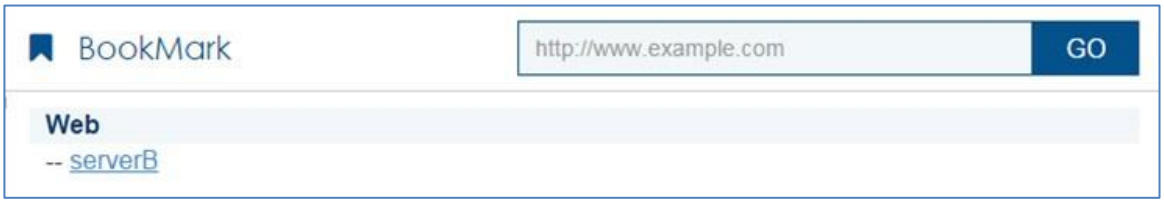
domainweb2を選択して、ログインページにアクセスします。

ログインページで、ユーザー名**sslvpnuser2**とパスワード**123456 TESTplat&!**を入力し、**Login**をクリックします。

図16 ログインページ

SSL VPNホームページが開き、ユーザーがアクセスできるWebリソースが**BookMark**領域に表示されます。この例では、図17に示すように、**serverB**が表示されます。**serverB**リンクをクリックして、サーバーBのWebリソースにアクセスします。

図17 SSL VPNゲートウェイのホームページ



#デバイス上のSSL VPNセッション情報を表示します。
[Device] display sslvpn session
Total users: 2

SSL VPN context: ctxweb1
Users: 1

Username	Connections	Idle time	Created	User IP
sslvpnuser1	6	0/00:00:23	0/00:00:23	40.1.1.1

SSL VPN context: ctxweb2
Users: 1

Username	Connections	Idle time	Created	User IP
sslvpnuser2	6	0/00:00:03	0/00:00:03	50.1.1.1

例:CA署名付き証明書を使用したWebアクセスの設定

ネットワーク構成

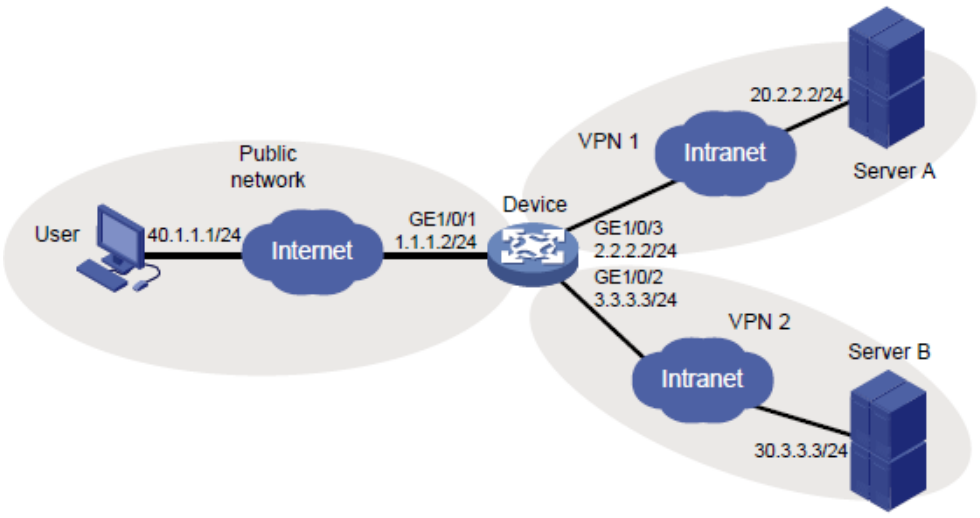
図18に示すように、デバイスは、パブリックネットワークとプライベートネットワークVPN 1およびVPN 2を接続するSSL VPNゲートウェイとして機能します。サーバーAとサーバーBは内部Webサーバーです。サーバーAはポート80でHTTPを使用します。サーバーBはポート443でHTTPSを使用します。

デバイスは、CA署名付きSSLサーバー証明書を使用します。

ユーザーがVPN 1のサーバーAおよびVPN 2のサーバーBにアクセスできるように、デバイスでSSL VPN Webアクセスを設定します。

ユーザーのローカル認証および認可を実行するようにデバイスを設定します。

図18 ネットワークダイアグラム



手順

1. デバイス上のインターフェースのIPアドレスを設定します(詳細は省略)。
2. VPNインスタンスを作成し、インターフェースをVPNインスタンスにバインドします(詳細は省略)。
3. デバイスのCA証明書ファイル**ca.cer**およびローカル証明書ファイル**server.pfx**を取得します(詳細は省略)。
4. デバイスとユーザー、デバイスとサーバーA、およびデバイスとサーバーBが相互に到達できることを確認します(詳細は省略)。
5. PKIドメインを設定します。

   #PKIドメインsslvpnを設定します。

   <Device> system-view

   [Device] pki domain sslvpn

   [Device-pki-domain-sslvpn] public-key rsa general name sslvpn

   [Device-pki-domain-sslvpn] undo crl check enable

   [Device-pki-domain-sslvpn] quit

   #CA証明書ファイル**ca.cer**とローカル証明書ファイル**server.pfx**をPKIドメインsslvpnにインポートします。

   [Device] pki import domain sslvpn der ca filename ca.cer

   [Device] pki import domain sslvpn p12 local filename server.pfx
6. sslという名前のSSLサーバーポリシーを作成し、そのポリシーにPKIドメインsslvpnを指定します。

   [Device] ssl server-policy ssl

   [Device-ssl-server-policy-ssl] pki-domain sslvpn

   [Device-ssl-server-policy-ssl] quit
7. SSL VPNゲートウェイを設定します。

   #SSL VPNゲートウェイgwのIPアドレスを1.1.1.2に、ポート番号を2000に設定し、サーバーポリシーsslをゲートウェイに適用します。

   [Device] sslvpn gateway gw

   [Device-sslvpn-gateway-gw] ip address 1.1.1.2 port 2000

   [Device-sslvpn-gateway-gw] ssl server-policy ssl

   #SSL VPNゲートウェイgwをイネーブルにします。

   [Device-sslvpn-gateway-gw] service enable

   [Device-sslvpn-gateway-gw] quit
8. SSL VPNコンテキストを設定します。

   #SSL VPNコンテキストctx1を作成し、コンテキストにゲートウェイgwとドメインdomain1を指定してから、コンテキストをVPNインスタンスVPN1に関連付けます。

   [Device] sslvpn context ctx1

[Device-sslvpn-context-ctx1] gateway gw domain domain1

[Device-sslvpn-context-ctx1] vpn-instance VPN1

#urlitemという名前のURL項目を作成し、そのURL項目にリソースURLを指定します。

[Device-sslvpn-context-ctx1] url-item urlitem

[Device-sslvpn-context-ctx1-url-item-urlitem] url http://20.2.2.2

[Device-sslvpn-context-ctx1-url-item-urlitem] quit

#SSL VPNコンテキストctx1にurllistという名前のURLリストを作成します。

[Device-sslvpn-context-ctx1] url-list urllist

#URLリストの見出しをwebに設定します。

[Device-sslvpn-context-ctx1-url-list-urllist] heading web

#URLアイテムurlitemをURLリストurllistに割り当てます。

[Device-sslvpn-context-ctx1-url-list-urllist] resources url-item urlitem

[Device-sslvpn-context-ctx1-url-list-urllist] quit

#SSL VPNコンテキストctx1用にpgroupという名前のSSL VPNポリシーグループを作成し、Webアクセス用のURLリストurllistを指定します。

[Device-sslvpn-context-ctx1] policy-group pgroup

[Device-sslvpn-context-ctx1-policy-group-pgroup] resources url-list urllist

[Device-sslvpn-context-ctx1-policy-group-pgroup] quit

#SSL VPNポリシーグループpgroupをデフォルトのポリシーグループとして指定します。

[Device-sslvpn-context-ctx1] default-policy-group pgroup

#SSL VPNコンテキストctx1をイネーブルにします。

[Device-sslvpn-context-ctx1] service enable

[Device-sslvpn-context-ctx1] quit

#SSL VPNコンテキストctx2を作成し、コンテキストにゲートウェイgwとドメインdomain2を指定して、コンテキストをVPNインスタンスVPN2に関連付けます。

[Device] sslvpn context ctx2

[Device-sslvpn-context-ctx2] gateway gw domain domain2

[Device-sslvpn-context-ctx2] vpn-instance VPN2

#urlitemという名前のURL項目を作成し、そのURL項目にリソースURLを指定します。

[Device-sslvpn-context-ctxweb1] url-item urlitem

[Device-sslvpn-context-ctxweb1-url-item-urlitem] url http://30.3.3.3

[Device-sslvpn-context-ctxweb1-url-item-urlitem] quit

#SSL VPNコンテキストctx2にurllistという名前のURLリストを作成します。

[Device-sslvpn-context-ctx2] url-list urllist

#URLリストの見出しをwebに設定します。

[Device-sslvpn-context-ctx2-url-list-urllist] heading web

#URLアイテムurlitemをURLリストurllistに割り当てます。

[Device-sslvpn-context-ctxweb1-url-list-urllist] resources url-item urlitem

[Device-sslvpn-context-ctxweb1-url-list-urllist] quit

#SSL VPNコンテキストctx2に対してpgroupという名前のSSL VPNポリシーグループを作成しWebアクセス用のURLリストurllistです。

[Device-sslvpn-context-ctx2] policy-group pgroup

[Device-sslvpn-context-ctx2-policy-group-pgroup] resources url-list urllist

[Device-sslvpn-context-ctx2-policy-group-pgroup] quit

#SSL VPNポリシーグループpgroupをデフォルトのポリシーグループとして指定します。

[Device-sslvpn-context-ctx2] default-policy-group pgroup

#SSL VPNコンテキストctx2をイネーブルにします。

[Device-sslvpn-context-ctx2] service enable

[Device-sslvpn-context-ctx2] quit

9. **sslvpn**という名前のローカルユーザーを作成し、パスワードを**123456 TESTplat&!**に設定し、サービスタイプを**sslvpn**、およびネットワークオペレータへのユーザーロール。ユーザーにポリシーグループ**pgroup**の使用を許可します。

   [Device] local-user sslvpn class network

   [Device-luser-network-sslvpn] password simple 123456TESTplat&!

   [Device-luser-network-sslvpn] service-type sslvpn

   [Device-luser-network-sslvpn] authorization-attribute user-role network-operator

   [Device-luser-network-sslvpn] authorization-attribute sslvpn-policy-group pgroup

   [Device-luser-network-sslvpn] quit

設定の確認

#デバイスでSSL VPNゲートウェイ**gw**が起動していることを確認します。

[Device] display sslvpn gateway

Gateway name: gw

  Operation state: Up

  IP: 1.1.1.2 Port: 2000

  SSL server policy configured: ssl

  SSL server policy in use: ssl

  Front VPN instance: Not configured

#SSL VPNコンテキストctx1およびctx2がデバイスでアップしていることを確認します。

[Device] display sslvpn context

Context name: ctx1

 Operation state: Up

 AAA domain: Not specified Certificate

authentication: Disabled Password
authentication: Enabled Authentication
use: All
Code verification: Disabled
Default policy group: pgroup
Associated SSL VPN gateway:
gw
Domain name: domain1
SSL client policy configured: ssl
SSL client policy in use: ssl
Maximum users allowed: 1048575
VPN instance: VPN1
Idle timeout: 30 min
Denied client types: Browsers

Context name: ctx2
Operation state: Up
AAA domain: Not specified Certificate
authentication: Disabled Password
authentication: Enabled Authentication
use: All
Code verification: Disabled
Default policy group: pgroup
Associated SSL VPN gateway:
gw
Domain name: domain2
SSL client policy configured: ssl
SSL client policy in use: ssl
Maximum users allowed: 1048575
VPN instance: VPN2
Idle timeout: 30 min
Denied client types: Browsers

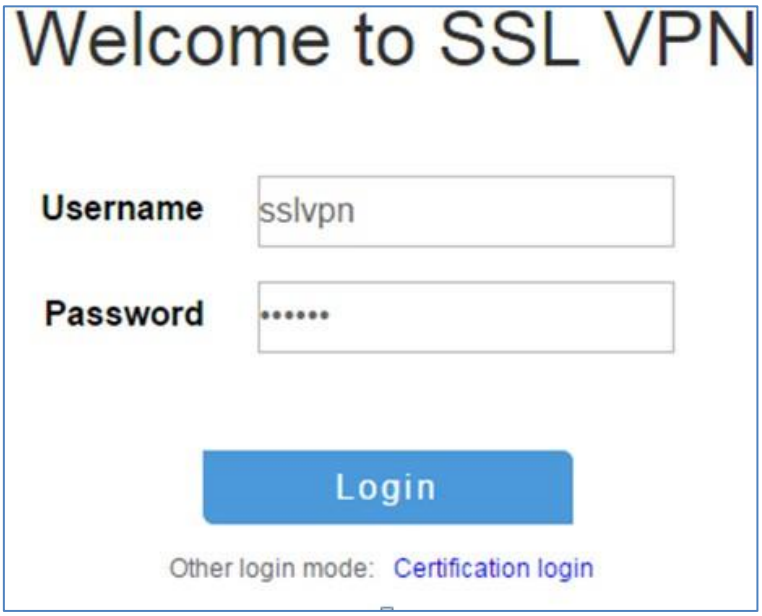
#ユーザーのコンピュータで、ブラウザのアドレスバーに**https://1.1.1.2:2000/**と入力して、ドメインリストページを開きます。

図19 ドメインリストページ

domain1を選択して、ログインページに入ります。

ログインページで、ユーザー名**sslvpn**とパスワード**123456 TESTplat&!**を入力しLoginをクリックします。

図20 ログインページ



#ユーザーのログイン後に、デバイス上のSSL VPNセッション情報を表示します。

[Device] display sslvpn session context ctx1

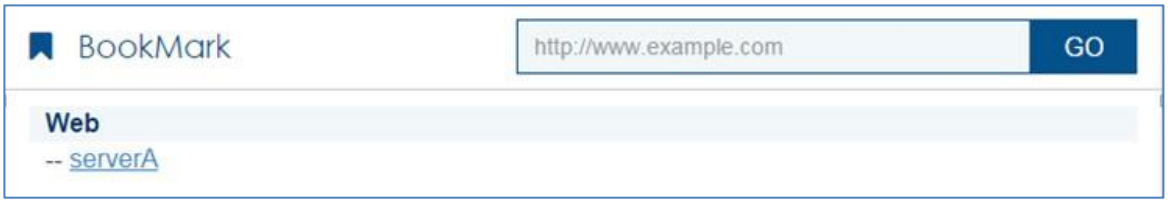
SSL VPN context: ctx1

Users: 1

Username	Connections	Idle time	Created	User IP
sslvpn	6	0/00:12:05	0/00:04:14	40.1.1.1

#SSL VPNゲートウェイのホームページで、**BookMark**領域の**serverA**リンクをクリックして、サーバーAのWebページを開きます。URL **https://1.1.1.2:2000/_proxy2/http/80/20.2.2.2/**がブラウザのアドレスバーに表示されます。

図21 SSL VPNゲートウェイのホームページ



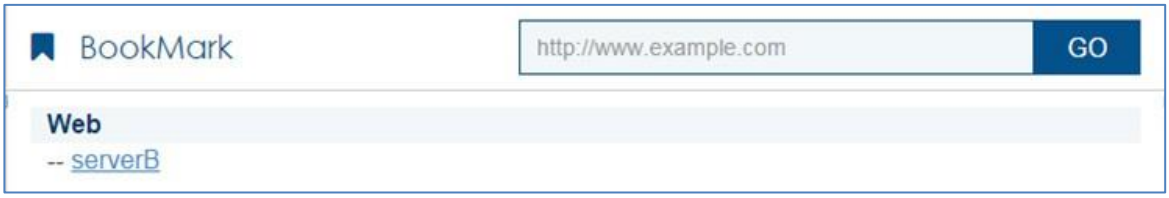
#ログアウトし、ブラウザを再起動します。**https://1.1.1.2:2000/**と入力してドメインリストページに入り、**domain2**を選択してログインページに入ります。ログインページで、ユーザー名**sslvpn**とパスワード**123456 TESTplat&!**を入力し、**Login**をクリックします(詳細は省略)。

#ユーザーのログイン後に、デバイス上のSSL VPNセッション情報を表示します。

```
[Device] display sslvpn session context       ctx2
SSL VPN context: ctx2
Users: 1
Username        Connections  Idle time       Created         User IP
sslvpn          6            0/00:02:05      0/00:01:11      40.1.1.1
```

#SSL VPNゲートウェイのホームページで、**BookMark**領域の**serverB**リンクをクリックして、サーバーBのWebページを開きます。URL **https://1.1.1.2:2000/_proxy2/https/443/30.3.3.3/**がブラウザのアドレスバーに表示されます。

図22 SSL VPNゲートウェイのホームページ



例:自己署名証明書を使用したTCPアクセスの設定

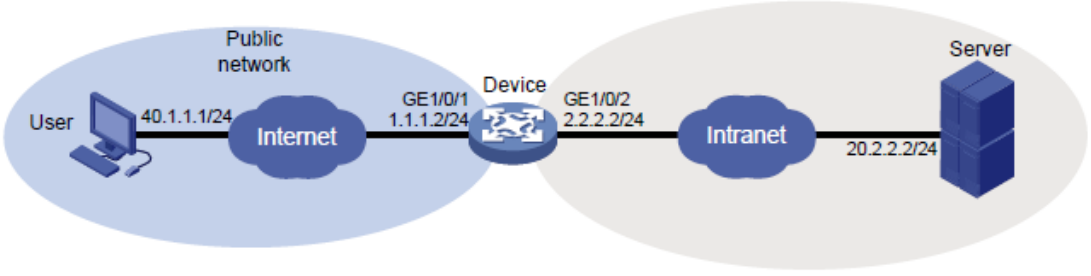
ネットワーク構成

図23に示すように、デバイスは、パブリックネットワークとプライベートネットワークを接続するSSL VPNゲートウェイとして機能します。

デバイスは、自己署名SSLサーバー証明書を使用します。

ユーザーが内部Telnetサーバーにアクセスできるように、デバイス上でSSL VPN TCPアクセスを設定します。ユーザーに対してローカル認証およびローカル認可を実行するようにデバイスを設定します。

図23 ネットワークダイアグラム



前提条件

ユーザーのPCを使用してSSL VPNゲートウェイ(デバイス)にアクセスする前に、PCにJava実行環境がインストールされていることを確認します。

手順

1. デバイス上のインターフェースのIPアドレスを設定します(詳細は省略)。
2. デバイスとユーザー、およびデバイスとサーバーが相互に通信できることを確認します(詳細は省略)。
3. SSL VPNゲートウェイを設定します。

   #SSL VPNゲートウェイgwのIPアドレスを1.1.1.2に、ポート番号を4430に設定します。

   <Device> system-view

   [Device] sslvpn gateway gw

   [Device-sslvpn-gateway-gw] ip address 1.1.1.2 port 4430

   #SSL VPNゲートウェイgwをイネーブルにします。

   [Device-sslvpn-gateway-gw] service enable

   [Device-sslvpn-gateway-gw] quit
4. SSL VPNコンテキストを設定します。

   #SSL VPNコンテキスト**ctxtcp**を作成し、コンテキストのゲートウェイ**gw**およびドメイン**domaintcp**を指定します。

   [Device] sslvpn context ctxtcp

   [Device-sslvpn-context-ctxtcp] gateway gw domain domaintcp

   #pfitemという名前のポート転送アイテムを作成します。

   [Device-sslvpn-context-ctxtcp] port-forward-item pfitem

   #内部サーバードレス20.2.2.2とポート23をローカルアドレス127.0.0.23とローカルポート2323にマッピングするポートフォワーディングインスタンスを作成します。

   [Device-sslvpn-context-ctxtcp-port-forward-item-pfitem] local-port 2323 local-name 127.0.0.23 remote-server 20.2.2.2 remote-port 23

   [Device-sslvpn-context-ctx-port-forward-item-pfitem1] quit

   #**pflist**という名前のポート転送リストを作成し、ポート転送アイテム**pfitem**をポート転送リストに割り当てます。

   [Device-sslvpn-context-ctxtcp] port-forward pflist

   [Device-sslvpn-context-ctxtcp-port-forward-pflist] resources port-forward-item pfitem

   [Device-sslvpn-context-ctxtcp-port-forward-pflist] quit

   #resourcegrpという名前のSSL VPNポリシーグループを作成し、ポート転送リストpflistをこのグループに割り当てます。

   [Device-sslvpn-context-ctxtcp] policy-group resourcegrp

[Device-sslvpn-context-ctxtcp-policy-group-resourcegrp] resources port-forward pflist

[Device-sslvpn-context-ctxtcp-policy-group-resourcegrp] quit

#SSL VPNコンテキストctxtcpをイネーブルにします。

[Device-sslvpn-context-ctxtcp] service enable

[Device-sslvpn-context-ctxtcp] quit

5. sslvpnuserという名前のローカルユーザーを作成し、パスワードを123456 TESTplat&!に、サービスタイプをsslvpnに、ユーザーロールをnetwork-operatorに設定します。ユーザーにポリシーグループresourcegrpの使用を許可します。

[Device] local-user sslvpnuser class network

[Device-luser-network-sslvpnuser] password simple 123456TESTplat&!

[Device-luser-network-sslvpnuser] service-type sslvpn

[Device-luser-network-sslvpnuser] authorization-attribute sslvpn-policy-group resourcegrp

[Device-luser-network-sslvpnuser] authorization-attribute user-role

network-operator

[Device-luser-network-sslvpnuser] quit

設定の確認

#デバイスでSSL VPNゲートウェイgwが起動していることを確認します。

[Device] display sslvpn gateway

Gateway name: gw

Operation state: Up IP:

1.1.1.2 Port: 4430

Front VPN instance: Not configured

#SSL VPNコンテキスト**ctx**がデバイスでアップしていることを確認します。

[Device] display sslvpn context

Context name: ctxtcp

Operation state: Up

AAA domain: Not specified Certificate

authentication: Disabled Password

authentication: Enabled Authentication

use: All

Code verification: Disabled

Default policy group: Not configured Associated

SSL VPN gateway: gw

Domain name: domaintcp

Maximum users allowed:

1048575 VPN instance: Not

configured Idle timeout: 30 min

Denied client types: Browsers

#ユーザーのコンピュータで、ブラウザのアドレスバーに**https://1.1.1.2:4430/**と入力して、ドメインリストページを開きます。

注:

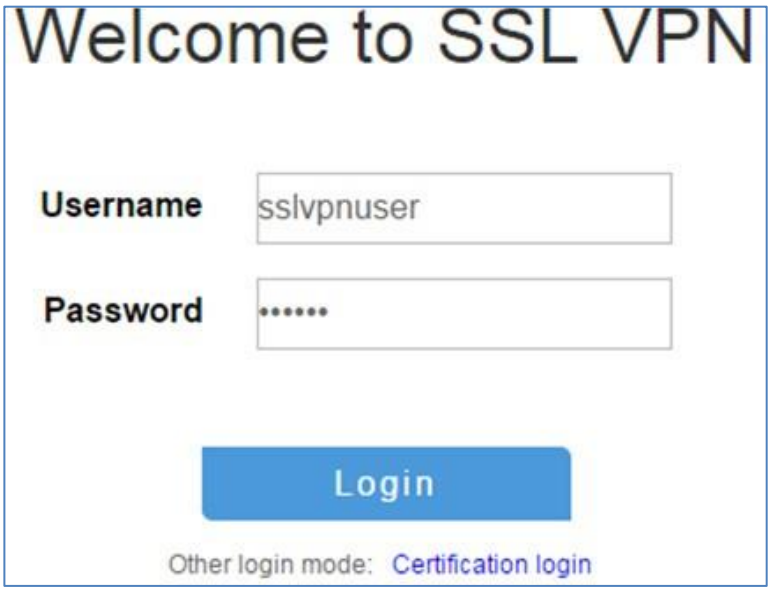
SSL VPNゲートウェイは自己署名のSSLサーバー証明書を使用するため、ゲートウェイにアクセスしようとすると、ブラウザに証明書が信頼されていないというエラーが表示されます。ゲートウェイへのアクセスを続行するには、を選択します。

図24 ドメインリストページ

domaintcpを選択して、ログインページにアクセスします。

ログインページで、ユーザー名**sslvpnuser**とパスワード**123456 TESTplat&!**を入力して**Login**をクリックします。

図25 ログインページ



#開いたSSL VPNホームページで、Startをクリックして TCPクライアントアプリケーションをダウンロードし、アプリケーションを起動します。

注:

TCPクライアントアプリケーションをダブルクリックして起動することはできません。

#PC上のローカルアドレス(127.0.0.1)およびローカルポート(2323)にTelnetします。ユーザーはサーバーにリモートアクセスできます(詳細は省略)。

#デバイス上のSSL VPNセッション情報を表示します。

[Device] display sslvpn session

Total users: 1

SSL VPN context: ctxtcp

Users: 1

Username	Connections	Idle time	Created	User IP
sslvpnuser	5	0/00:00:51	0/00:17:26	40.1.1.1

#デバイス上のSSL VPNポート転送接続情報を表示します。

[Device] display sslvpn session

Total users: 1

SSL VPN context: ctxtcp

Users: 1

Username	Connections	Idle time	Created	User IP
sslvpnuser	5	0/00:00:51	0/00:17:26	40.1.1.1

例:CA署名付き証明書を使用したTCPアクセスの設定

ネットワーク構成

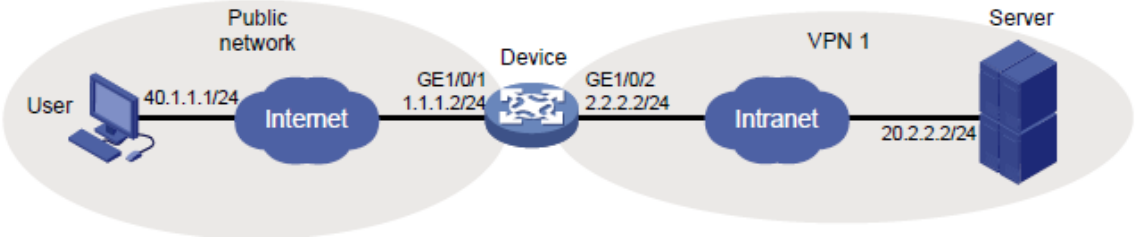
図26に示すように、デバイスは、パブリックネットワークとプライベートネットワークVPN 1を接続するSSL VPNゲートウェイとして機能します。

デバイスは、CA署名付きSSLサーバー証明書を使用します。

ユーザーがVPN 1の内部Telnetサーバーにアクセスできるように、デバイス上でSSL VPN TCPアクセスを設定します。

ユーザーのローカル認証およびローカル認可を実行するように、デバイスを設定します。

図26 ネットワークダイアグラム



前提条件

ユーザーのPCを使用してSSL VPNゲートウェイ(デバイス)にアクセスする前に、PCにJava実行環境がインストールされていることを確認します。

手順

1. デバイス上のインターフェースのIPアドレスを設定します(詳細は省略)。

2. VPNインスタンスを作成し、GigabitEthernet 1/0/2をVPNインスタンスにバインドします(詳細は省略)。
3. デバイスのCA証明書ファイルca.cerおよびローカル証明書ファイル**server.pfx**を取得します(詳細は省略)。
4. デバイスとユーザー、およびデバイスとサーバーが相互に通信できることを確認します(詳細は省略)。
5. PKIドメインを設定します。

   #PKIドメインsslvpnを設定します。

   <Device> system-view

   [Device] pki domain sslvpn

   [Device-pki-domain-sslvpn] public-key rsa general name sslvpn

   [Device-pki-domain-sslvpn] undo crl check enable

   [Device-pki-domain-sslvpn] quit

   #CA証明書ファイルca.cerとローカル証明書ファイルserver.pfxをPKIドメインsslvpnにインポートします。

   [Device] pki import domain sslvpn der ca filename ca.cer

   [Device] pki import domain sslvpn p12 local filename server.pfx
6. sslという名前のSSLサーバーポリシーを作成し、そのポリシーにPKIドメインsslvpnを指定します。

   [Device] ssl server-policy ssl

   [Device-ssl-server-policy-ssl] pki-domain sslvpn

   [Device-ssl-server-policy-ssl] quit
7. SSL VPNゲートウェイを設定します。

   #SSL VPNゲートウェイgwのIPアドレスを1.1.1.2に、ポート番号を2000に設定し、サーバーポリシーsslをゲートウェイに適用します。

   [Device] sslvpn gateway gw

   [Device-sslvpn-gateway-gw] ip address 1.1.1.2 port 2000

   [Device-sslvpn-gateway-gw] ssl server-policy ssl

   #SSL VPNゲートウェイgwをイネーブルにします。

   [Device-sslvpn-gateway-gw] service enable

   [Device-sslvpn-gateway-gw] quit
8. SSL VPNコンテキストを設定します。

   #SSL VPNコンテキストctxを作成し、コンテキストにゲートウェイgwを指定してから、コンテキストをVPNインスタンスVPN1に関連付けます。

   [Device] sslvpn context ctx

   [Device-sslvpn-context-ctx] gateway gw

   [Device-sslvpn-context-ctx] vpn-instance VPN1

#pfitem1という名前のポート転送項目を作成します。

[Device-sslvpn-context-ctx] port-forward-item pfitem1

#内部サーバードレス20.2.2.2とポート23をローカルアドレス127.0.0.1とローカルポート2323にマッピングするポートフォワーディングインスタンスを作成します。

[Device-sslvpn-context-ctx-port-forward-item-pfitem1] local-port 2323 local-name 127.0.0.1 remote-server 20.2.2.2 remote-port 23 description telnet

[Device-sslvpn-context-ctx-port-forward-item-pfitem1] quit

#plistという名前のポート転送リストを作成し、ポート転送アイテムpfitem1をポート転送リストに割り当てます。

[Device-sslvpn-context-ctx] port-forward plist

[Device-sslvpn-context-ctx-port-forward-plist] resources port-forward-item pfitem1

[Device-sslvpn-context-ctx-port-forward-plist] quit

#pgroupという名前のSSL VPNポリシーグループを作成し、ポート転送リストplistをグループに割り当てます。

[Device-sslvpn-context-ctx] policy-group pgroup

[Device-sslvpn-context-ctx-policy-group-pgroup] resources port-forward plist

[Device-sslvpn-context-ctx-policy-group-pgroup] quit

#SSL VPNコンテキストctxをイネーブルにします。

[Device-sslvpn-context-ctx] service enable

[Device-sslvpn-context-ctx] quit

9. **sslvpn**という名前のローカルユーザーを作成し、パスワードを**123456 TESTplat&!**に設定し、サービスタイプを**sslvpn**、およびユーザーロールを**network-operator**に設定します。ユーザーにポリシーグループ**pgroup**の使用を許可します。

   [Device] local-user sslvpn class network

   [Device-luser-network-sslvpn] password simple 123456TESTplat&!

   [Device-luser-network-sslvpn] service-type sslvpn

   [Device-luser-network-sslvpn] authorization-attribute user-role network-operator

   [Device-luser-network-sslvpn] authorization-attribute sslvpn-policy-group pgroup

   [Device-luser-network-sslvpn] quit

設定の確認

#デバイスでSSL VPNゲートウェイgwが起動していることを確認します。

[Device] display sslvpn gateway

Gateway name: gw

Operation state: Up IP:

1.1.1.2 Port: 2000

SSL server policy configured: ssl

SSL server policy in use: ssl Front

VPN instance: Not configured

#SSL VPNコンテキストctxがデバイスでアップしていることを確認します。

[Device] display sslvpn context

Context name: ctx

Operation state: Up

AAA domain: Not specified Certificate

authentication: Disabled Password

authentication: Enabled Authentication

use: All

Code verification: Disabled

Default policy group: Not configured Associated

SSL VPN gateway: gw

SSL client policy configured: ssl

SSL client policy in use: ssl

Maximum users allowed: 1048575

VPN instance: VPN1

Idle timeout: 30 min

Denied client types: Browsers

#ユーザーのコンピュータで、ブラウザのアドレスバーにhttps://1.1.1.2:2000/と入力して、ログインページに入ります。

#ログインページで、ユーザー名sslvpnとパスワード123456 TESTplat&!を入力して**Login**をクリックします。

図27 ログインページ

開いたSSL VPNホームページで、Startをクリックして TCPクライアントアプリケーションをダウンロードし、アプリケーションを起動します。

注:
TCPクライアントアプリケーションをダブルクリックして起動することはできません。

PC上のローカルアドレス(127.0.0.1)およびローカルポート(2323)にTelnetします。ユーザーはサーバーにリモートアクセスできます(詳細は省略)。

#デバイス上のSSL VPNセッション情報を表示します。

[Device] display sslvpn session context ctx SSL

VPN context: ctx

Users: 1

Username	Connections	Idle time	Created	User IP
sslvpn	6	0/00:12:05	0/00:04:14	40.1.1.1

#デバイス上のSSL VPNポート転送接続情報を表示します。

[Device] display sslvpn port-forward connection SSL

VPN context : ctx

Client address : 40.1.1.1
Client port : 50788
Server address : 20.2.2.2
Server port : 23
State : Connected

例:自己署名証明書を使用したIPアクセスの設定

ネットワーク構成

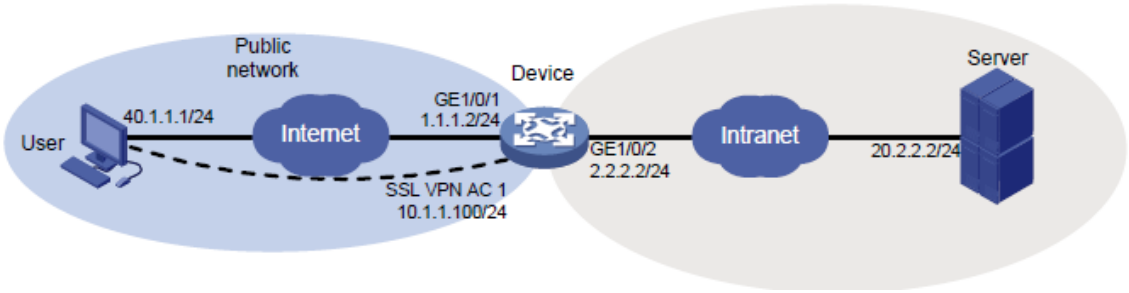
図28に示すように、デバイスは、パブリックネットワークとプライベートネットワークを接続するSSL VPNゲートウェイとして機能します。

デバイスは、自己署名SSLサーバー証明書を使用します。

デバイスでSSL VPN IPアクセスを設定して、ユーザーがプライベートネットワーク内の内部サーバーにアクセスできるようにします。

ユーザーのローカル認証および認可を実行するようにデバイスを設定します。

図28ネットワークダイアグラム



前提条件

IPアクセスを設定する前に、サーバーに10.1.1.0/24へのルートがあることを確認してください。

手順

1. デバイス上のインターフェースのIPアドレスを設定します(詳細は省略)。
2. デバイスとユーザー、およびデバイスとサーバーが相互に通信できることを確認します(詳細は省略)。
3. SSL VPNゲートウェイを設定します。

   #SSL VPNゲートウェイgwのIPアドレスを1.1.1.2に、ポート番号を4430に設定します。

   <Device> system-view

   [Device] sslvpn gateway gw

   [Device-sslvpn-gateway-gw] ip address 1.1.1.2 port 4430

   #SSL VPNゲートウェイgwをイネーブルにします。

   [Device-sslvpn-gateway-gw] service enable

   [Device-sslvpn-gateway-gw] quit
4. sslvpnpoolという名前のIPアクセスアドレスプールを作成し、アドレス範囲を10.1.1.1から10.1.1.10。

   [Device] sslvpn ip address-pool sslvpnpool 10.1.1.1 10.1.1.10
5. SSL VPN ACインターフェースAC 1を作成し、このインターフェースのIPアドレスを10.1.1.100/24に設定します。

[Device] interface sslvpn-ac 1

[Device-SSLVPN-AC1] ip address 10.1.1.100 24

[Device-SSLVPN-AC1] quit

6. SSL VPNコンテキストを設定します。

#SSL VPNコンテキストctxipを作成し、ゲートウェイgwとドメインdomainipをコンテキストに指定します。

[Device] sslvpn context ctxip

[Device-sslvpn-context-ctxip] gateway gw domain domainip

#IPアクセス用のインターフェースSSL VPN AC 1を指定します。

[Device-sslvpn-context-ctxip] ip-tunnel interface sslvpn-ac 1

#rtlistという名前のルートリストを作成し、ルート20.2.2.0/24をリストに追加します。

[Device-sslvpn-context-ctxip] ip-route-list rtlist

[Device-sslvpn-context-ctxip-route-list-rtlist] include 20.2.2.0 24

[Device-sslvpn-context-ctxip-route-list-rtlist] quit

#IPアクセス用のアドレスプールsslvpnpoolを指定します。

[Device-sslvpn-context-ctxip] ip-tunnel address-pool sslvpnpool mask 24

#resourcegrpという名前のSSL VPNポリシーグループを作成し、IPアクセスにルートリストrtlistを指定してから、IPアクセスフィルタリングにACL 3000を指定します。

[Device-sslvpn-context-ctxip] policy-group resourcegrp

[Device-sslvpn-context-ctxip-policy-group-resourcegrp] ip-tunnel access-route ip-route-list rtlist

[Device-sslvpn-context-ctxip-policy-group-resourcegrp] filter ip-tunnel acl 3000

[Device-sslvpn-context-ctxip-policy-group-resourcegrp] quit

#SSL VPNコンテキストctxをイネーブルにします。

[Device-sslvpn-context-ctxip] service enable

[Device-sslvpn-context-ctxip] quit

#ACL 3000を作成します。サブネット10.1.1.0/24から発信され、宛先が20.2.2.0/24のパケットを許可するルールを追加します。

[Device] acl advanced 3000

[Device-acl-ipv4-adv-3000] rule permit ip source 10.1.1.0 0.0.0.255 destination 20.2.2.0 0.0.0.255

[Device-acl-ipv4-adv-3000] quit

7. sslvpnuserという名前のローカルユーザーを作成し、パスワードを123456 TESTplat&!に、サービスタイプをsslvpnに、ユーザーロールをnetwork-operatorに設定します。ユーザーにポリシーグループresourcegrpの使用を許可します。

[Device] local-user sslvpnuser class network

[Device-luser-network-sslvpnuser] password simple 123456TESTplat&!

[Device-luser-network-sslvpnuser] service-type sslvpn

[Device-luser-network-sslvpnuser] authorization-attribute sslvpn-policy-group resourcegrp

[Device-luser-network-sslvpnuser] authorization-attribute user-role network-operator

[Device-luser-network-sslvpnuser] quit

設定の確認

#デバイスでSSL VPNゲートウェイgwが起動していることを確認します。

[Device] display sslvpn gateway

Gateway name: gw

Operation state: Up IP:

1.1.1.2 Port: 4430

Front VPN instance: Not configured

#デバイスでSSL VPNコンテキストctxipが起動していることを確認します。

[Device] display sslvpn context

Context name: ctxip

Operation state: Up

AAA domain: Not specified Certificate

authentication: Disabled Password

authentication: Enabled Authentication

use: All

Code verification: Disabled

Default policy group: Not configured Associated

SSL VPN gateway: gw

Domain name: domainip

Maximum users allowed:

1048575 VPN instance: Not

configured Idle timeout: 30 min

Denied client types: Browsers

#ユーザーのコンピュータで、ブラウザのアドレスバーにhttps://1.1.1.2:4430/と入力して、ドメインリストページを開きます。

注:

SSL VPNゲートウェイは自己署名のSSLサーバー証明書を使用するため、ゲートウェイにアクセスしようとすると、ブラウザに証明書が信頼されていないというエラーが表示されます。ゲートウェイへのアクセスを続行するには、を選択します。

図29 ドメインリストページ

ログインページにアクセスするには、domainipを選択します。

ログインページで、ユーザー名sslvpnuserとパスワード123456 TESTplat&!を入力し**Login**をクリックします。

図30 ログインページ

開いたSSL VPNホームページで、Startをクリックして IPクライアントアプリケーションをダウンロードし、インストールします。

IPクライアントアプリケーションがインストールされたら、図31に示すようにiNodeクライアントを起動します。

図31 iNodeクライアントの起動

図32に示すように、Connectをクリックして SSL VPNクライアントにログインします。

図32 SSL VPNクライアントへのログイン

#ユーザーがサーバーに対してpingを実行できることを確認します。

C:\>ping 20.2.2.2

Pinging 20.2.2.2 with 32 bytes of data:

Reply from 20.2.2.2: bytes=32 time=31ms TTL=254

Reply from 20.2.2.2: bytes=32 time=18ms TTL=254

Reply from 20.2.2.2: bytes=32 time=15ms TTL=254

Reply from 20.2.2.2: bytes=32 time=16ms TTL=254

Ping statistics for 20.2.2.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 15ms, Maximum = 31ms, Average = 20ms

#デバイス上のSSL VPNセッション情報を表示します。

[Device] display sslvpn session user sslvpnuser

User	:	sslvpnuser ctxip	
Context	:	resourcegrp	
Policy group	:	30 min	
Idle timeout	:		
Created at	:	16:38:48 UTC Wed	07/26/2017
Lastest	:	16:47:41 UTC Wed	07/26/2017
User IPv4 address	:	172.16.1.16	
Allocated IP	:	10.1.1.1	
Session ID	:	14	
Web browser/OS	:	Windows	

署名付き証明書を使用したIPアクセスの設定

ネットワーク構成

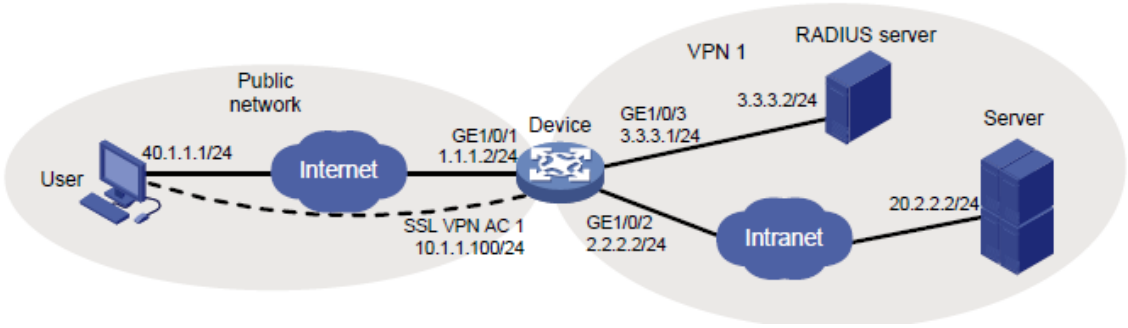
図33に示すように、デバイスは、パブリックネットワークとプライベートネットワークVPN 1を接続するSSL VPNゲートウェイとして機能します。

デバイスは、CA署名付きSSLサーバー証明書を使用します。

ユーザーがVPN 1の内部サーバーにアクセスできるように、デバイス上でSSL VPN IPアクセスを設定します。

ユーザーに対して(リモートRADIUSサーバーを介して)リモート認証および認可を実行するようにデバイスを設定します。

図33 ネットワークダイアグラム



前提条件

IPアクセスを設定する前に、次の作業を実行します。

- サーバーに10.1.1.0/24へのルートがあることを確認します。
- ユーザーに認証と認可を提供するようにRADIUSサーバーを設定します。

手順

1. デバイス上のインターフェースのIPアドレスを設定します(詳細は省略)。
2. VPNインスタンスを作成し、GigabitEthernet 1/0/2をVPNインスタンスにバインドします(詳細は省略)。
3. デバイスのCA証明書ファイルca.cerおよびローカル証明書ファイルserver.pfxを取得します(詳細は省略)。
4. デバイスとユーザー、およびデバイスとサーバーが相互に通信できることを確認します(詳細は省略)。
5. PKIドメインを設定します。

   #PKIドメインsslvpnを設定します。

   <Device> system-view

   [Device] pki domain sslvpn

   [Device-pki-domain-sslvpn] public-key rsa general name sslvpn

   [Device-pki-domain-sslvpn] undo crl check enable

   [Device-pki-domain-sslvpn] quit

   #CA証明書ファイルca.cerとローカル証明書ファイルserver.pfxをPKIドメインsslvpnにインポートします。

   [Device] pki import domain sslvpn der ca filename ca.cer

   [Device] pki import domain sslvpn p12 local filename server.pfx
6. sslという名前のSSLサーバーポリシーを作成し、そのポリシーにPKIドメインsslvpnを指定します。

   [Device] ssl server-policy ssl

   [Device-ssl-server-policy-ssl] pki-domain sslvpn

   [Device-ssl-server-policy-ssl] quit

7. SSL VPNゲートウェイを設定します。

#SSL VPNゲートウェイgwのIPアドレスを1.1.1.2に、ポート番号を2000に設定し、サーバーポリシーsslをゲートウェイに適用します。

[Device] sslvpn gateway gw

[Device-sslvpn-gateway-gw] ip address 1.1.1.2 port 2000

[Device-sslvpn-gateway-gw] ssl server-policy ssl

#SSL VPNゲートウェイgwをイネーブルにします。

[Device-sslvpn-gateway-gw] service enable

[Device-sslvpn-gateway-gw] quit

8. ippoolという名前のIPアクセスアドレスプールを作成し、アドレス範囲を10.1.1.1～10.1.1.10に指定します。

[Device] sslvpn ip address-pool ippool 10.1.1.1 10.1.1.10

9. SSL VPN ACインターフェースAC 1を作成し、このインターフェースをVPNインスタンスVPN1にバインドして、このインターフェースのIPアドレスを10.1.1.100/24に設定します。

[Device] interface sslvpn-ac 1

[Device-SSLVPN-AC1] ip binding vpn-instance VPN1

[Device-SSLVPN-AC1] ip address 10.1.1.100 24

[Device-SSLVPN-AC1] quit

10. SSL VPNコンテキストを設定します。

#SSL VPNコンテキストctxを作成し、コンテキストにゲートウェイgwを指定してから、コンテキストをVPNインスタンスVPN1に関連付けます。

[Device] sslvpn context ctx

[Device-sslvpn-context-ctx] gateway gw

[Device-sslvpn-context-ctx] vpn-instance VPN1

#SSL VPNコンテキストctxで、SSL VPNユーザーのAAAにISPドメインdomain1を指定します。

[Device-sslvpn-context-ctx] aaa domain domain1

#rtlistという名前のルートリストを作成し、ルート20.2.2.0/24をリストに追加します。

[Device-sslvpn-context-ctx] ip-route-list rtlist

[Device-sslvpn-context-ctx-route-list-rtlist] include 20.2.2.0 255.255.255.0

[Device-sslvpn-context-ctx-route-list-rtlist] quit

#uriaclという名前のURI ACLを作成し、icmp://20.2.2.0へのアクセスを許可するルールをACLに追加します。

[Device-sslvpn-context-ctx] uri-acl uriacl

[Device-sslvpn-context-ctx-uri-acl-uriacl] rule 1 permit uri icmp://20.2.2.0

[Device-sslvpn-context-ctx-uri-acl-uriacl] quit

#IPアクセス用のインターフェースSSL VPN AC 1を指定します。

[Device-sslvpn-context-ctx] ip-tunnel interface sslvpn-ac 1

#IPアクセス用のアドレスプールippoolを指定します。

[Device-sslvpn-context-ctx] ip-tunnel address-pool ippool mask 255.255.255.0

#pgroupという名前のSSL VPNポリシーグループを作成し、IPアクセスにルートリストrtlistを指定してから、IPアクセスフィルタリングにURI ACL uriaclを指定します。

[Device-sslvpn-context-ctx] ip-tunnel address-pool ippool mask 255.255.255.0

[Device-sslvpn-context-ctx] policy-group pgroup

[Device-sslvpn-context-ctx-policy-group-pgroup] ip-tunnel access-route ip-route-list rtlist

[Device-sslvpn-context-ctx-policy-group-pgroup] filter ip-tunnel uri-acl uriacl

[Device-sslvpn-context-ctx-policy-group-pgroup] quit

#SSL VPNコンテキストctxをイネーブルにします。

[Device-sslvpn-context-ctx] service enable

[Device-sslvpn-context-ctx] quit

11. RADIUS設定を構成します。

#rschemeという名前のRADIUSスキームを作成します。プライマリ認証サーバーとプライマリアカウンティングサーバーを3.3.3.2に指定します。サーバーとの通信用のキーを123456に設定します。

[Device] radius scheme rscheme

[Device-radius-rscheme] primary authentication 3.3.3.2

[Device-radius-rscheme] primary accounting 3.3.3.2

[Device-radius-rscheme] accounting-on enable

[Device-radius-rscheme] key authentication simple 123456

[Device-radius-rscheme] key accounting simple 123456

#RADIUSサーバーに送信されるユーザー名からドメイン名を除外します。

[Device-radius-rscheme] user-name-format without-domain

[Device-radius-rscheme] quit

12. group1という名前のユーザーグループを作成し、そのユーザーグループにSSL VPNポリシーグループpgroupの使用を許可します。

[Device] user-group group1

[Device-ugroup-group1] authorization-attribute sslvpn-policy-group pgroup

[Device-ugroup-group1] quit

13. domain1という名前のISPドメインを作成し、ユーザーグループgroup1を使用する権限をドメインに付与します。

[Device] domain domain1

[Device-isp-domain1] authorization-attribute user-group group1

#ユーザーのAAAにRADIUSスキームrschemeを使用するようにISPドメインを設定します。

[Device-isp-domain1] authentication sslvpn radius-scheme rscheme

[Device-isp-domain1] authorization sslvpn radius-scheme rscheme

[Device-isp-domain1] accounting sslvpn radius-scheme rscheme

[Device-isp-domain1] quit

設定の確認

#デバイスでSSL VPNゲートウェイgwが起動していることを確認します。

[Device] display sslvpn gateway

Gateway name: gw

Operation state: Up IP:

1.1.1.2 Port: 2000

SSL server policy configured: ssl

SSL server policy in use: ssl Front

VPN instance: Not configured

#SSL VPNコンテキストctxがデバイスでアップしていることを確認します。

[Device] display sslvpn context

Context name: ctx

Operation state: Up

AAA domain: domain1

Certificate authentication: Disabled Password

authentication: Enabled Authentication use: All

Code verification: Disabled

Default policy group: Not configured

Associated SSL VPN gateway: gw

SSL client policy configured: ssl

SSL client policy in use: ssl

Maximum users allowed: 1048575

VPN instance: VPN1

Idle timeout: 30 min

Denied client types: Browsers

#ユーザーのコンピュータで、IPアクセスクライアントソフトウェアを起動し、アドレス1.1.1.2、ポート番号2000、ユーザー名sslvpn、およびパスワード123456 TESTplat&!を入力して、SSL VPNゲートウェイにログインします(詳細は省略)。

#デバイス上のSSL VPNセッション情報を表示します。

[Device] display sslvpn session context ctx SSL

VPN context: ctx

Users: 1

Username	Connections	Idle time	Created	User IP
sslvpn	6	0/00:02:05	0/00:03:14	40.1.1.1

#ユーザーPCで、IPv4ルーティングテーブルを表示して、ユーザーがサーバーへのルートを持っていることを確認します。

注:

アドレス40.1.1.1/24はローカルNICのアドレスであり、10.1.1.1/24はSSL VPNゲートウェイがユーザーに割り当てるアドレスです。

>route -4 print IPv4

Route Table

==========

Active Routes:

Network Destination	Netmask	Gateway	Interface	Metric
10.1.1.0	255.255.255.0	On-link	10.1.1.1	276
10.1.1.1	255.255.255.255	On-link	10.1.1.1	276
10.1.1.255	255.255.255.255	On-link	10.1.1.1	276
20.2.2.0	255.255.255.0	On-link	10.1.1.1	276
20.2.2.255	255.255.255.255	On-link	10.1.1.1	276
40.1.1.0	255.255.255.0	On-link	40.1.1.1	276
40.1.1.1	255.255.255.255	On-link	40.1.1.1	276
40.1.1.255	255.255.255.255	On-link	40.1.1.1	276

==========

#ユーザーがサーバーに対してpingを実行できることを確認します。

C:\>ping 20.2.2.2

Pinging 20.2.2.2 with 32 bytes of data:

Reply from 20.2.2.2: bytes=32 time=197ms TTL=254

Reply from 20.2.2.2: bytes=32 time=1ms TTL=254

Reply from 20.2.2.2: bytes=32 time=1ms TTL=254

Reply from 20.2.2.2: bytes=32 time=186ms TTL=254

Ping statistics for 20.2.2.2:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate

round trip times in milli-seconds:

Minimum = 1ms, Maximum = 197ms, Average = 96ms