KTest

更に上のクオリティ　更に上のサービス

問題集

http://www.ktest.jp

1年で無料進級することに提供する

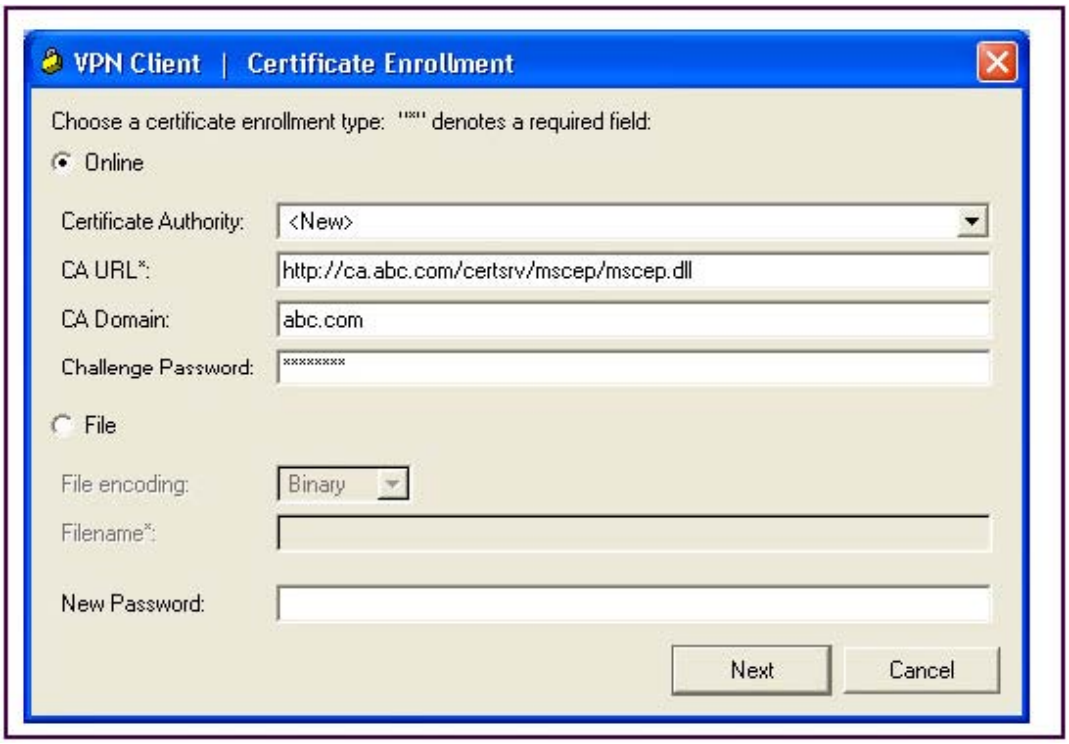
Exam : **642-648**

Title : Deploying Cisco ASA VPN Solutions (VPN v2.0)

Version : DEMO

1. どのステートメントは、信頼されたネットワーク検出（TND）機能に関する正しいですか？
A. シスコの AnyConnect3.0 クライアントは、Windows、Mac、および Linux プラットフォームで TND をサポートしています。
B. TND と、エンドポイントでの Cisco Secure Desktop の基本的なスキャンのつの結果は、デバイスが信頼のメンバーまたは信頼できないネットワークであるかどうかを判断することです。
C. 有効になっており、CSD スキャンホストが信頼できないネットワークのメンバーであると判断した場合、管理者は、Cisco AnyConnect の VPN クライアントを起動するからエンドユーザーを禁止する TND 機能を設定することができます。
D. ユーザが企業ネットワーク内にあるとき、TND を自動的にシスコの AnyConnect セッションを切断するように構成することができます。
Answer: D
Explanation:
http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect25/administration/guide/ac03features.html
トラステッドネットワークの検出
トラステッドネットワーク検出（TND）は、ユーザーが企業ネットワーク（信頼できないネットワーク）の外にあるときの AnyConnect は自動的に VPN 接続をユーザが企業ネットワーク（信頼できるネットワーク）内にあるときに VPN 接続を切断して起動する必要ができるようになります。この機能により、ユーザは信頼ネットワークの外にあるときに VPN 接続を開始することによって、より高いセキュリティ意識を奨励しています。
AnyConnect のもログオン（SBL）の前にスタートが実行され、ユーザが信頼できるネットワークに移動すると、コンピュータに表示さ SBL ウィンドウが自動的に閉じます。 TND を手動で VPN 接続を確立するユーザの能力を妨げない。これは、ユーザーが信頼されたネットワーク内で手動で開始することを VPN 接続を切断されません。ユーザーが最初に信頼されていないネットワークに接続して、信頼されたネットワークに移動した場合 TND のみ VPN セッションを切断します。ユーザーが自宅で VPN 接続を行い、その後、企業のオフィスに移動した場合、例えば、TND は、VPN セッションを切断します。
TND 機能は AnyConnect の GUI を制御し、自動的に接続を開始しているので、GUI はすべての回で実行する必要があります。ユーザーが終了する GUI をした場合、TND、自動的に VPN 接続を開始しません。あなたがの AnyConnect プロファイルで TND 構成します。変更は ASA コンフィギュレーションに必要ありません。

2. 展示を参照してください。



あなたは、認証にデジタル証明書を使用する Cisco VPN クライアント、ラップトップを設定している。どのプロトコルの Cisco VPN Client は、CA サーバからデジタル証明書を取得するために使用しますか?

A. FTP
B. LDAP
C. HTTPS
D. SCEP
E. OCSP

Answer: D

Explanation:

http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/cert_cfg.html

About CRLs

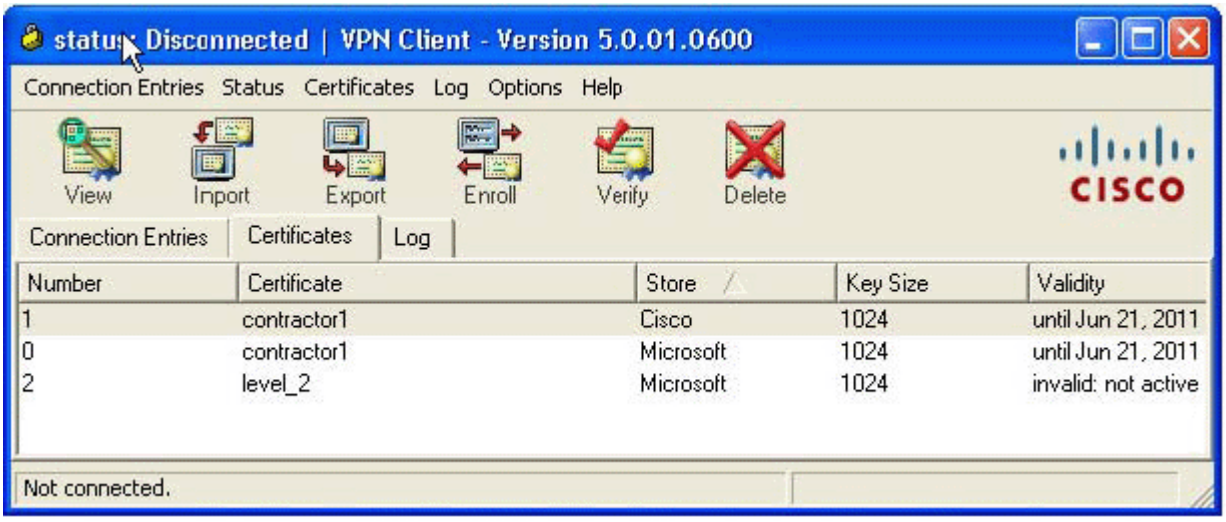
証明書失効リストは、有効期間内の証明書が発行元の CA によって無効にされているかどうかを判定する手段の 1 つに、セキュリティアプライアンスを提供します。 CRL の設定は、トラストポイントのコンフィギュレーションの一部です。

あなたが証明書（CRL コマンドを失効チェック）認証するときに必ず CRL チェックを行うようにセキュリティアプライアンスを設定できます。また、CA が更新された CRL データを提供するために使用できない場合、証明書認証が成功することができますなしの引数（取り消しチェック CRL none コマンド）を追加することにより CRL チェックはオプションにすることができます。セキュリティアプライアンスは HTTP、SCEP、または LDAP を使用して CA のから CRL を取得することができます。トラストポイントごと取り出された CRL は、トラストポイントごとに設定可能な時間の長さのためにキャッシュされます。セキュリティアプライアンスは、それがキャッシュ CRL のように構成されている時間の長さ以上にキャッシュされた CRL を持っている場合、セキュリティアプライアンスは、信頼性の高い、または"陳腐"であるには余りにも古い CRL を考慮する。セキュリティアプライアンスが CRL 証明書認証が古い CRL をチェックする必要があります次回の新しいバージョンを取得しようとします。

3. クライアントレス SSL VPN を使用する場合は、Cisco ASA アプライアンスを通過するためにいくつ

かのアプリケーションや Web リソースを望んでいない可能性があります。これらのアプリケーションや Web リソースについては、Cisco ASA の管理者としては、どの設定を使うべきでしょうか?
A. スプリットトンネリング用の Cisco ASA アプライアンスを設定します。
B. SSL VPN のカスタマイズエディタでネットワークアクセスの例外を設定します。
C. コンテンツリライトを無効にするには、Cisco ASA アプライアンスを設定します。
D. URL エントリのバイパスをイネーブルにするには、Cisco ASA アプライアンスを設定します。
E. Cisco ASA のアプライアンスのプロキシ機能をバイパスするスマートトンネルを設定します。
Answer: C
Explanation:
http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/user/guide/vpn_web.html
コンテンツリライト
コンテンツリライトペインには、コンテンツのリライトを有効にするか無効にされているすべてのアプリケーションが一覧表示されます。クライアントレス SSL VPN は、JavaScript など、VBScript では、Java、およびユーザが使用しているかどうかに応じて異なる意味とアクセス制御規則を持っているかもしれプロキシ HTTP トラフィックへのマルチバイト文字などの高度な要素を含むコンテンツ変換/書き換えエンジンを介して、アプリケーショントラフィックを処理 SSL VPN デバイス内または独立のアプリケーション。
デフォルトでは、セキュリティアプライアンスは、書き換え、または、すべてのクライアントレストラフィックを変換します。セキュリティアプライアンスを通過するためにいくつかのアプリケーションや Web リソース（例えば、公開 Web サイト）たくない場合があります。セキュリティアプライアンスは、そのため、ユーザーは、セキュリティアプライアンスを経由せずに、特定のサイトやアプリケーションをブラウズしてみましょうリライトルールを作成することができます。これは、IPSec VPN 接続でのスプリットトンネリングと類似しています。
あなたは、複数の書き換えルールを作成することができます。ルール番号は、セキュリティアプライアンスの検索が最低で始まる、注文番号でルールを書き換えるため重要であり、それが一致する最初のルールを適用します。

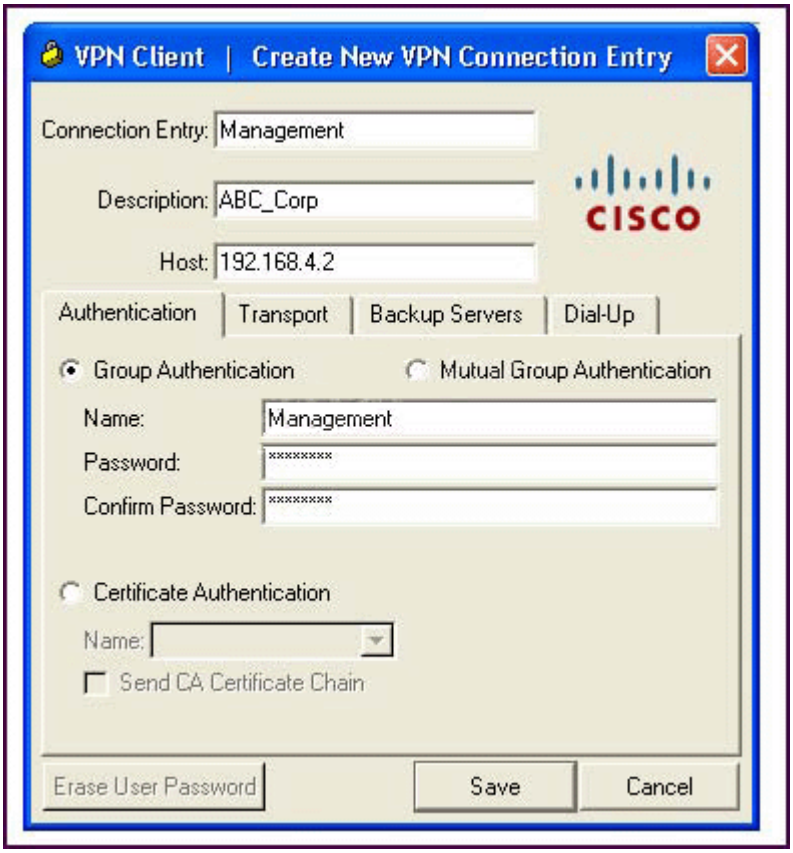
4. 展示を参照してください。



"LEVEL_2"デジタル証明書は、ラップトップにインストールしました。
何が"無効なアクティブではありません"のステータスメッセージを引き起こす可能性がありますか?
A. 最初の使用時に、CA のパスフレーズをサーバが提供証明書を検証するために入力されます。

B. それは、その最初の使用時にピアデバイスによって検証されるまで、"新しくインストールされた"デジタル証明書がアクティブになりません。
C. ユーザは、Cisco VPN Client 内検証ボタンをクリックしていません。
D. CA サーバとラップトップ PC のクロックが同期していません。
Answer: D
Explanation:
http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/cert_cfg.html
証明書には、日付と、それらが有効で期限が切れることになっている時間がある。セキュリティアプライアンスが CA に登録し、証明書を取得すると、セキュリティアプライアンスは現在の時刻が証明書の有効範囲内にあることをチェックします。それがその範囲外にある場合、登録は失敗する。同じことは、ASA と PC の間の通信に適用されます。

5. 展示を参照してください。



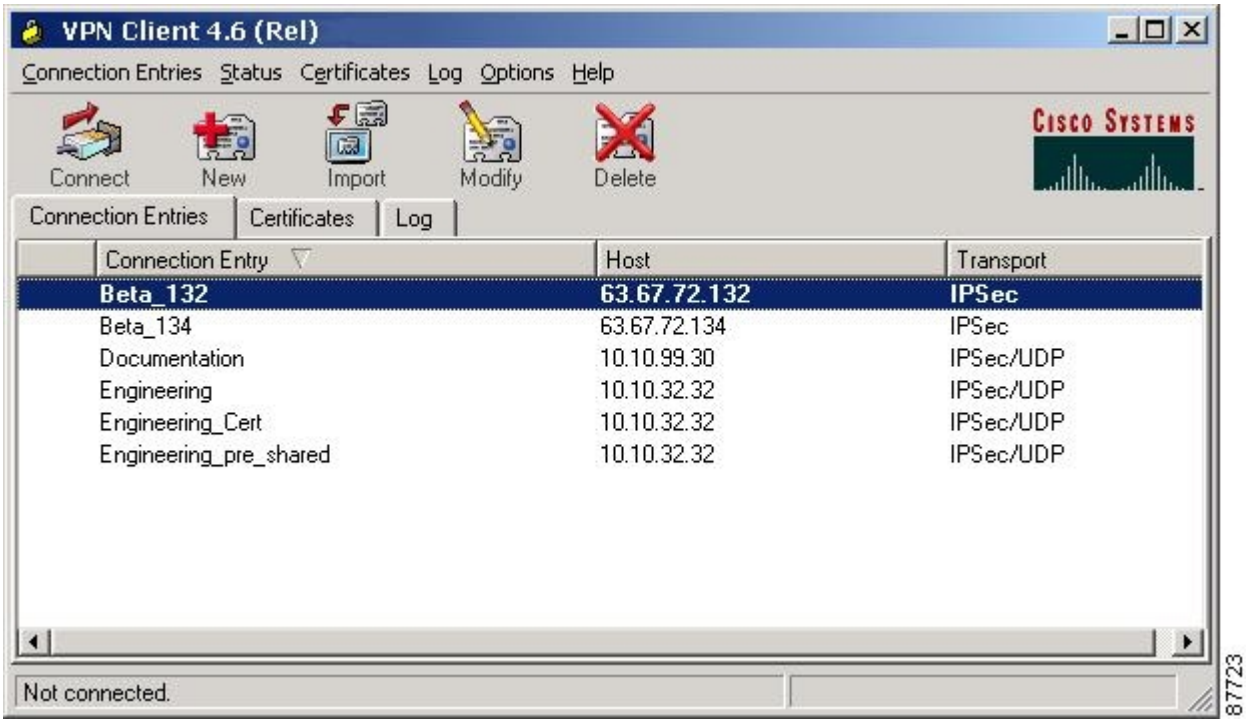
NOC エンジニアが作成新しい VPN 接続エントリの各フィールドに情報を入力する過程にある。
どのステートメントが正常にこれを行う方法を説明しますか？
A. それが Cisco ASA アプライアンスに指定されている接続エントリフィールドで、接続プロファイルの名前を入力します。
B. Host フィールドに、リモートクライアント装置の IP アドレスを入力してください。
C. 認証タブで、グループ認証または対称事前共有キー認証を有効にするには、相互グループ認証のラジオボタンをクリックします。
D. それが Cisco ASA アプライアンスに指定されている名前フィールドに、接続プロファイルの名前を入力します。
Answer: D

Explanation:

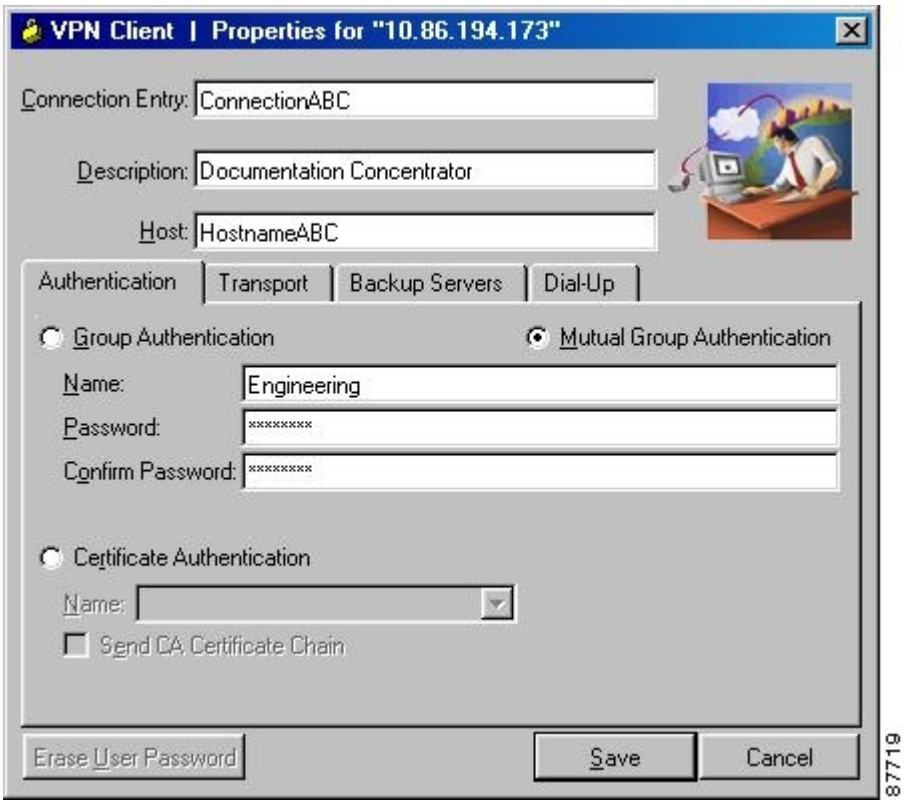
http://www.cisco.com/en/US/docs/security/vpn_client/cisco_vpn_client/vpn_client46/win/user/guide/vc4.html#wp1074766

ステップ1> [プログラム]> [Cisco SystemsのVPNクライアント> VPN Clientを起動し選択することで、VPN Clientを起動します。

ステップ2 VPN Clientアプリケーションが起動し、アドバンストモードのメインウィンドウ（図4¬1）が表示されます。あなたがそこにすでにない場合は、シンプルモードの[オプション]メニューを開き、[詳細モードか、またはCtrl-Mを選択します。

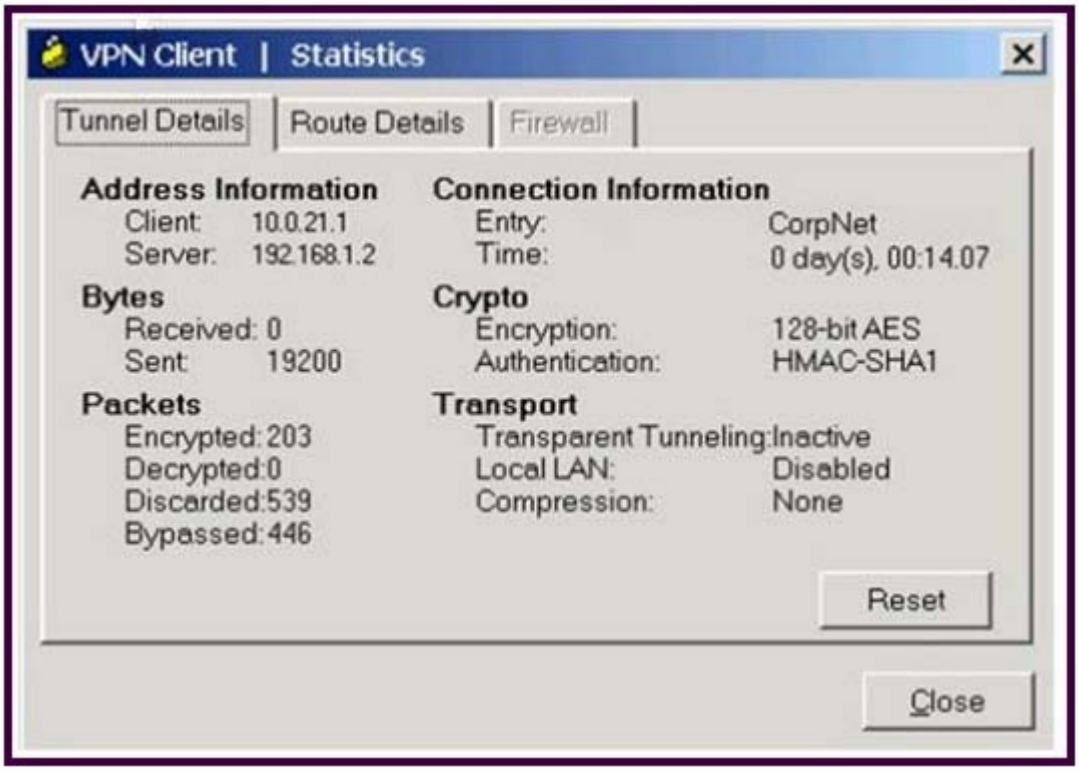


ステップ3ツールバーまたは接続エントリメニューから新規を選択します。 VPN Clientは、フォームを表示します。



ステップ 4 この新しい接続に固有の名前を入力します。例えば、エンジニアリング、この接続を識別する任意の名前を使用できます。この名前にはスペースを含めることができ、そしてそれは、大文字と小文字は区別されません。ステップ 5 この接続の説明を入力します。このフィールドはオプションですが、それはさらにこの接続を識別するのに役立ちます。たとえば、エンジニアリングリモートサーバへの接続。 6 は、アクセスしたいリモート VPN 装置のホスト名または IP アドレスを入力します。
グループ認証は、ネットワーク管理者は、通常、あなたのためのグループ認証を設定します。これが事実でない場合は、次の手順を実行します。ステップ 1 グループ認証のラジオボタンをクリックします。Name フィールドにステップ 2、あなたが所属する IPSec グループの名前を入力します。このエントリでは、大文字と小文字が区別されます。
Password フィールドにステップ 3 は、IPSec グループのパスワード（これも大文字と小文字が区別される）を入力します。このフィールドには、アスタリスクしか表示されます。
4Confirm Password フィールドにもう一度入力してパスワードを確認するステップです。

6. 展示を参照してください。

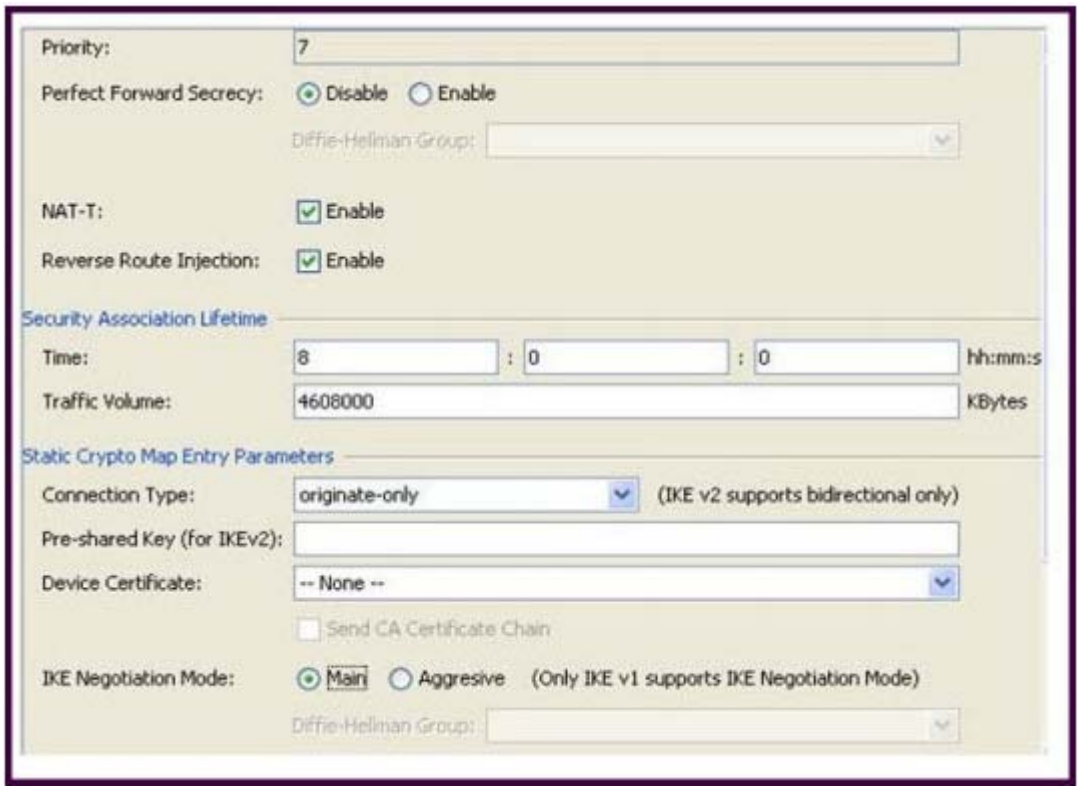


新しい NOC エンジニアは VPN 接続をトラブルシューティングします。
どちらの Cisco VPN Client の統計画面内のフィールドに関するステートメントが正しいですか?
A. 10.0.21.1 の ISP によって割り当てられた IP アドレスは PC の VPN アダプタに割り当てられています。
B. シスコの VPN クライアントが接続されているセキュリティアプライアンスの IP アドレスは 192.168.1.2 です。
C. CorpNet と、トンネルのパラメータ、接続が使用している Cisco ASA のグループポリシーの名前です。
D. 透過的にパケットを送信し、テスト目的のためにトンネルを介して暗号化されていないために、クライアントの能力がオフになっています。
E. スプリットトンネリングがイネーブルで、シスコの VPN クライアントは復号化されたパケットを登録しません。
Answer: B

7. XYZ 社のシステムエンジニアは、売上高は、ABC 本社に呼び出しながら、ファイアウォールの背後にある ABC 会議室から FTP 経由でデモを転送するために XYZ の販売デモ・フォルダにアクセスしようとしました。エンジニアは、リモートアクセス VPN トンネルを介して XYZ に達することができなかった。自宅から前日、しかし、エンジニアは、XYZ の販売デモ・フォルダに接続し、DSL 上の IPsec を経由してデモを移さなかった。
接続が動作するように取得し、デモンストレーションを転送するには、エンジニアは何をすべきでしょうか?
A. ケーブル伝送に DSL からの変化を考慮するために、IPSec クライアント上で MTU サイズを変更します。
B. IPSec クライアント上でローカル LAN アクセスオプションを有効にします。
C. IPsec のクライアントでの TCP オプションの上の IPsec を有効にします。
D. PC 上のクライアントレス SSL VPN オプションを有効にします。
Answer: C

Explanation:
伝送制御プロトコル（TCP）上の IP セキュリティ（IPSec）は、VPN Client がセキュリティプロトコル（ESP、プロトコル 50）またはインターネット鍵交換（IKE、ユーザー・データグラム・プロトコル（UDP）500）をカプセル化する標準では機能しないことができる環境で動作することができます、または既存のファイアウォールルールへの変更のみで機能することができます。 TCP 経由の IPSec は IKE と TCP パケット内の IPSec プロトコルの両方をカプセル化し、それは両方のネットワーク・アドレス変換（NAT）およびポートアドレス変換をトンネルセキュア可能（PAT）デバイスとファイアウォール。

8. 展示を参照してください。



サイトツーサイト VPN トンネルを構成する際、新しい NOC エンジニアは逆ルート注入パラメータを検出した。
スタティックルートは、ローカルの Cisco ASA で逆ルート注入を可能にしませんどのような効果、IGP への Cisco ASA によって再配布されていると仮定すると、コンフィギュレーションにありますか?
A. ローカル Cisco ASA は、サイトツーサイト VPN トンネルの遠隔端へのデフォルトルートをアドバタイズします。
B. ローカル Cisco ASA は、サイトツーサイト VPN トンネルの遠い端までローカル Cisco ASA 上で実行されているダイナミックルーティングプロトコルからのルートをアドバタイズします。
C. ローカル Cisco ASA は、サイトツーサイト VPN トンネルの遠端であるルートをアドバタイズします。
D. ローカル Cisco ASA は、サイトツーサイト VPN トンネルの遠隔端にサイトツーサイト VPN トンネルのその側にあるルートをアドバタイズします。
Answer: C

9. 展示を参照してください。

```
ASA5520# show vpn-session anyconnect
Username     : engineer1              Index        : 76
Assigned IP  : 10.0.4.80              Public IP    : 172.26.26.15
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 63506                  Bytes Rx     : 17216
Group Policy : engineering            Tunnel Group : contractor
Login Time   : 11:35:57 UTC Thu Jul 1 2011
Duration     : 0h:01m:52s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : Static                 VLAN         : 100
```

NOC エンジニアは、SSL VPN トンネルにいくつかのログイン前のパラメータを調整する必要があります。表示された情報から、どこにエンジニアはログイン前のセッション属性を見つけるに移動すべきですか？

A. "工学"グループポリシー

B. "請負業者"接続プロファイル

C. "engineer1"ローカル/ AAA ユーザー

D. DfltGrpPolicy グループポリシー

Answer: B

10. 展示を参照してください。

```
ASA5520# show vpn-session anyconnect
Username     : engineer1              Index        : 76
Assigned IP  : 10.0.4.80              Public IP    : 172.26.26.15
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 63506                  Bytes Rx     : 17216
Group Policy : engineering            Tunnel Group : contractor
Login Time   : 11:35:57 UTC Thu Jul 1 2011
Duration     : 0h:01m:52s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : Static                 VLAN         : 100
```

NOC エンジニアは、SSL VPN トンネルにいくつかの postlogin パラメータを調整する必要があります。情報が示されてから、どこにエンジニアはすべて postlogin セッションパラメータを見つけるために、に移動すべきですか？

A. "工学"グループポリシー

B. "請負業者"接続プロファイル

C. DefaultWEBVPNGroup グループポリシー

D. DefaultRAGroup グループポリシー

E. "engineer1"ローカル/ AAA ユーザー

Answer: A

Explanation:

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t11/htwebvpn.html#wp1054618

ポリシーグループは、リモートユーザーのグループ用に設定されているリソースのポータルと権限のプ

レゼンテーションを定義するコンテナです。 policy group コマンドを入力するの webvpn グループポリシーコンフィギュレーションモードでルータを配置。それを構成した後、グループポリシーがデフォルトグループポリシーコマンドを設定することにより、SSL VPN コンテキスト設定に取り付けられている。次のタスクは、この構成で実現されている：

11. 展示を参照してください。

ABC 社は、NOC のメンバーは、Cisco WebVPN のログインページ上のドロップダウンメニューからトンネルグループを選択する能力を必要とします。
Cisco ASA の管理者は、どのようにこのタスクを達成するでしょうか?
A. ログインページ上の名前付きグループに証明書の所有者へのアクセスを許可する証明書の OU フィールドで定義されている複数のグループとの特別なアイデンティティ証明書を、定義します。
B. グループポリシーの下では、ログインページに表示され、必要な個々のグループを包含し、デフォルトのグループを定義します。
C. 接続プロファイルの下では、ログインページに表示され、必要な個々のプロファイルを包含 NOC プロファイルを定義します。
D. 接続プロファイルの下で有効、"ユーザーが接続プロファイルを選択することができます。"
Answer: D
Explanation:
シスコ ASDM ユーザガイドバージョン 6.1 は、SSL VPN 接続の追加]または編集> 詳細> SSL VPN このダイアログボックスでは、リモートユーザーがログイン時に見ているものに影響する属性を設定できます。フィールド•ログインページれる事前設定のカスタマイズ属性を適用するために指定することで、ユーザのログインページのルックアンドフィールをカスタマイズは、設定します。デフォルトは DfltCustomization です。
•設定 GUI カスタマイゼーションオブジェクトウィンドウが管理開きます。テーブル内•接続エイリアスを一覧表示し、既存の接続エイリアスとそのステータスと、その表の項目を追加または削除することができます。接続は、ユーザーがログイン時に特定の接続（トンネルグループ）を選択できるように構成されている場合は接続エイリアスは、ユーザのログインページに表示されます。 - あなたが追加して接続エイリアスを有効にすることができている接続の追加エイリアスウィンドウを、追加で開きます。- 接

続エイリアステーブルから選択した行を削除し、削除します。確認も取り消しもありません。 •グループテーブルの既存のグループ URL とそのステータスの URL を一覧表示して、追加またはそのテーブルの項目を削除することができます。接続は、ユーザーがログイン時に特定のグループを選択できるように構成されている場合、グループの URL は、ユーザのログインページに表示されます。 - あなたが追加およびグループ URL を有効にすることができているグループの追加 URL ウィンドウを、追加で開きます。 - 接続エイリアステーブルから選択した行を削除し、削除します。確認も取り消しもありません。

12. 展示を参照してください。

```
access-list temp_acl webtype permit url http://10.0.4.10
webvpn
 enable outside
 svc enable
 tunnel-group-list enable
group-policy temp_worker internal
group-policy temp_worker attributes
 banner value Welcome Temp Workers!
 vpn-tunnel-protocol webvpn
 vlan 100
 webvpn
  url-list value Corporate_Server
  url-entry disable
group-policy Default attributes
 vpn-tunnel-protocol IPSec svc webvpn
 webvpn
  url-list value Corporate_Server
  filter value temp_acl
username temp1 password cisco
```

```
username temp1 attributes
 vpn-group-policy temp_worker
 vpn-tunnel-protocol webvpn
 group-lock value temp_worker
 service-type remote-access
 webvpn
  file-browsing disable
  file-entry enable
  url-entry disable
 hidden-shares none
  url-list value Corporate_Server
  customization value temp_worker
tunnel-group temp_worker type remote-access
tunnel-group temp_worker general-attributes
 default-group-policy temp_worker
tunnel-group temp_worker webvpn-attributes
 customization temp_worker
 group-alias temp_worker enable
 group-url https://192.168.4.2/temp_worker enable
```

ジュニアネットワークエンジニアは、新しい一時的な労働者を収容するために、企業の Cisco ASA アプライアンスを構成しました。セキュリティ上の理由から、IT 部門は、10.0.4.10 の IP アドレスを持つ企業のサーバーへの新しい一時的な労働者の内部ネットワークへのアクセスを制限したいと考えています。ジュニアネットワークエンジニアが設定を終えた後、IT セキュリティの専門家は、一時的な労働者のアカウントをテストしました。テスターは、一時的な労働者の WebVPN ユーザアカウントから追加の安全なサーバーの URL にアクセスすることができました。
ジュニアネットワークエンジニアは何を間違って設定したのですか?
A. ACL が正しく設定されています。
B. ACL が正しく適用されたか、適用されませんでした。
C. ネットワークブラウジングは、一時的な労働者のグループポリシーで制限されていません。
D. ネットワークブラウジングは、一時的な労働者のユーザポリシーで制限されていません。
Answer: B

13. 企業の財務部門は、そのいずれかのサーバー上で実行するための新しい非 Web ベースの TCP アプリケーションツールを購入しました。特定の金融の従業員が業務時間外中にソフトウェアへのリモートアクセスを必要とする。これらの従業員は自分の PC に"管理者"権限を持っていません。
このアプリケーションを実行できるように SSL VPN トンネルを設定するための正しい方法は何ですか?
A. アプリケーションのスマートトンネルを設定します。
B. 従業員、クライアントレス SSL VPN ポータルの "金融ツール" VNC ブックマークを設定します。
C. 設定プラグインが最適なアプリケーションに適合します。
D. SSL VPN トンネルが確立されるたびに金融従業員は、Cisco の AnyConnect SSL VPN クライアントを

ダウンロードするには、Cisco ASA アプライアンスを設定します。

Answer: A

Explanation:

http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/webvpn.html スマートトンネルはクライアントレス(ブラウザベース)経路などのセキュリティアプライアンスと SSL VPN セッション、プロキシサーバーなどのセキュリティアプライアンスを使用して、TCP ベースのアプリケーションとプライベートサイト間の接続です。あなたは、スマートトンネルアクセスを付与するためのアプリケーションを識別し、各アプリケーションへのローカルパスを指定することができます。 Microsoft Windows の上で動作するアプリケーションでは、あなたは、スマートトンネルアクセスを付与するための条件として、チェックサムの SHA-1 ハッシュの一致を必要とすることができます。 Lotus Sametime のと Microsoft Outlook Express は、スマートトンネルアクセスを付与する場合がありますへのアプリケーションの例です。スマートトンネルを設定すると、アプリケーションがクライアントであるか、または Web 対応アプリケーションであるかどうかに応じて、次のいずれかの手順を必要とする：

クライアントアプリケーションのいずれかまたは複数のスマートトンネルリストを作成してから、スマートトンネルアクセスを提供したい人のためのグループポリシーまたはローカルユーザポリシーにリストを割り当てる。

スマートトンネルアクセス対象 Web 対応アプリケーションの URL を指定する 1 つ以上のブックマークリストエントリを作成し、その後の DAP にリストを割り当てるには、スマートトンネルアクセスを提供したい人のためのグループポリシー、またはローカルユーザポリシー。また、クライアントレス SSL VPN セッションでスマートトンネル接続にログイン資格情報の提出を自動化するための Web 対応アプリケーションを一覧表示することができます。なぜスマートトンネル? スマートトンネルアクセスは、クライアントの TCP ベースのアプリケーションは、サービスに接続するために、ブラウザベースの VPN 接続を使用することができます。これは、ポートフォワーディング、プラグインや、レガシー技術に比べて、ユーザーに次のような利点を提供している：

スマートトンネルは、プラグインよりも優れたパフォーマンスを提供します。

ポート転送と異なり、スマートトンネルは、ローカルポートへのローカルアプリケーションのユーザ接続を必要としないことにより、ユーザーエクスペリエンスを簡素化します。

ポート転送と異なり、スマートトンネルは、ユーザーが管理者権限を持っている必要はありません。プラグインの利点は、クライアントアプリケーションがリモートコンピュータにインストールする必要がないということである。スマートトンネルの要件、制約事項、および制限事項は、次のセクションでは、スマートトンネルの要件と制限を分類。スマートトンネル一般要件と制限は、次の一般的な要件と制限がある：

または Mac OS 10.4 または 10.5、スマートトンネルを送信されるリモートホストは、Microsoft Windows Vista、Windows XP、または Windows 2000 の 32 ビットバージョンを実行している必要があります。

スマートトンネル自動サインオンは、Windows 上で Microsoft Internet Explorer だけをサポートしています。ブラウザは、Java、Microsoft の ActiveX の、またはその両方で有効にする必要があります。

スマートトンネルは、Microsoft Windows およびセキュリティアプライアンスを実行しているコンピュータの間に配置された唯一のプロキシをサポートしています。スマートトンネルは、Internet Explorer の設定を（つまり、Windows でシステム全体の使用のために意図されたものです）を使用します。リモートコンピュータがセキュリティアプライアンスに到達するためにプロキシサーバを必要とする場合は、接続の終端の URL は、プロキシサービスから除外する URL のリストでなければなりません。プロキシ設定は、ASA に向かうトラフィックがプロキシを通過するように指定されている場合、すべてのスマートトンネルトラフィックは、プロキシを経由します。

HTTP ベースのリモートアクセスのシナリオでは、時にはサブネットが VPN ゲートウェイへのユーザー

• アクセスを提供しません。この場合には、ウェブおよびエンドユーザの位置間でトラフィックをルーティングする ASA の前に配置プロキシは、Web アクセスを提供する。しかし、VPN ユーザだけは、ASA の前に置かれたプロキシを設定することができます。
その際、彼らはこれらのプロキシが CONNECT メソッドをサポートしていることを確認する必要があります。認証を必要とするプロキシの場合、スマートトンネルは基本的なダイジェスト認証タイプをサポートしています。
ブラウザプロセスが同じであればスマートトンネルが起動すると、デフォルトでは、セキュリティアプライアンスは、VPN セッションを介してすべてのブラウザトラフィックを渡します。トンネルのすべてのポリシーが適用される場合、セキュリティアプライアンスは、これを行います。ユーザがブラウザプロセスの別のインスタンスを起動する場合は、VPN セッションを介してすべてのトラフィックを渡します。ブラウザプロセスが同じで、セキュリティアプライアンスは、URL へのアクセスを提供しない場合、ユーザはそれを開くことができません。回避策として、トンネルすべてではありません、トンネルポリシーを割り当てます。
ステートフルフェールオーバーでは、スマートトンネル接続を保持しません。ユーザーは、フェイルオーバー後に再接続する必要があります。

14. どのプラグインに関する声明は false ですか？
A. プラグインは、リモートシステム上の任意のインストールを必要としません。
B. プラグインは、リモートシステムの管理者権限が必要です。
C. プラグインのサポートインタラクティブ端末アクセスをします。
D. プラグインは、Windows Mobile プラットフォームでサポートされていません。
Answer: B
Explanation:
http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deployhtml#wp1162435
プラグイン
セキュリティアプライアンスは、クライアントレス SSL VPN 接続用の Java プラグインをサポートしています。プラグインはブラウザで動作する Java プログラムです。これらのプラグインは、SSH / Telnet の、RDP、VNC、および Citrix が含まれています。それらに変更を加えずに、GNU 一般公衆利用許諾契約書あたり（GPL）、シスコの再配布はプラグイン。
GPL あたり、シスコが直接これらのプラグインを強化することができません。プラグインを使用するには、Java ランタイム環境（JRE）1.4.2.x 以降をインストールする必要があります。また、ここで指定された互換性のあるブラウザを使用する必要がある：
http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpncompatibility.html

15. 一時的な労働者は、社内サーバー、projects.xyz.com サーバのコンソールにアクセスするために、SSH プラグインとクライアントレス SSL VPN を使用する必要があります。セキュリティ上の理由から、ネットワークセキュリティ監査人は一時的なユーザーは 1 社内サーバー、10.0.4.18 に制限されていると主張する。あなたは、一時的なユーザのネットワークアクセスを担当していますネットワークエンジニアです。
一つ projects.xyz.com サーバーへの SSH アクセスを制限するために何をすべきですか？
A. アクセスリスト temp_user_acl 拡張許可 TCP 任意のホスト 10.0.4.18 式 22 を設定します。
B. アクセスリスト temp_user_acl 標準許可ホスト 10.0.4.18 式 22 を設定します。
C. アクセスリスト temp_acl webtype 許可された URL に ssh:/ /10.0.4.18 を設定します。

D. プラグインは、SSH ブックマークホスト 10.0.4.18 のためにを設定し、ネットワークが一時的な労働者のクライアントレス SSL VPN ポータルにブラウジングを無効にします。

Answer: C

Explanation: ウェブの ACL

ウェブの ACL テーブルはクライアントレス SSL VPN トラフィックに適用されるセキュリティアプライアンスで設定フィルタが表示されます。以下の表は、それぞれのアクセス制御リスト（ACL）の名前と、が表示され、ACL 名、ACL に割り当てられたアクセス制御エントリ（ACE）の右側にインデント。各 ACL には、許可または拒否するアクセス許可を、または特定のネットワーク、サブネット、ホスト、および Web サーバへのアクセスを拒否します。各 ACE は、ACL の機能を果たす一つのルールを指定します。あなたは、クライアントレス SSL VPN トラフィックに適用する ACL を設定できます。次のルールが適用されます•あなたは、任意のフィルタを設定しない場合、すべての接続が許可されます。 •セキュリティアプライアンスは、インターフェイスのインバウンド ACL のみをサポートしています。 •各 ACL の最後には、、表記されない暗黙のルールが明示的に許可されていないすべてのトラフィックを拒否します。あなたは Webtype アクセスリストエントリに複数のワイルドカードを定義するには、次のワイルドカード文字を使用することができます：•ない文字または任意の数の文字に一致しないようにアスタリスク"*"を入力してください。 •疑問符を入力してください"? "正確に任意の 1 文字に一致する。 •範囲内の任意の 1 文字に一致する範囲演算子を作成するために"[]"の角括弧を入力してください。次の例では、Webtype アクセスリストにワイルドカードを使用する方法を示しています。など•次の例では、一致した URLhttp://www.cisco.com/ and http://wwz.caco.com/: access-list test webtype permit url http://ww?.c*co*/

16. クライアントレス SSL VPN の認可とは、ユーザがクライアントレス SSL VPN セッション内で実行できるアクションを定義します。どのステートメントは、SSL VPN の認証処理に関する正しいですか？

A. リモートクライアントは、外部 AAA サーバ上に設定されているダイナミックアクセスポリシーを適用することにより、認可することができます。

B. リモートクライアントは、外部データベースからグループパラメータを適用することにより、外部から承認されることができます。

C. リモートクライアント認証は、RADIUS および TACACS+プロトコルによってサポートされています。

D. 外部認可を設定するには、プロキシカットスルーのための Cisco ASA を設定する必要があります。

Answer: B

17. VPN ウィザードを経由してリモートアクセス IPsec トンネルを追加した後、管理者は、IPsec ポリシーのパラメータを調整する必要があります。

シスコ ASDM で IPsec ポリシーパラメータを調整するための正しい場所はどこですか？

A. IPsec のユーザープロファイル

B. クリプトマップ

C. グループポリシー

D. IPsec のポリシー

E. IKE ポリシー

Answer: B

Explanation:

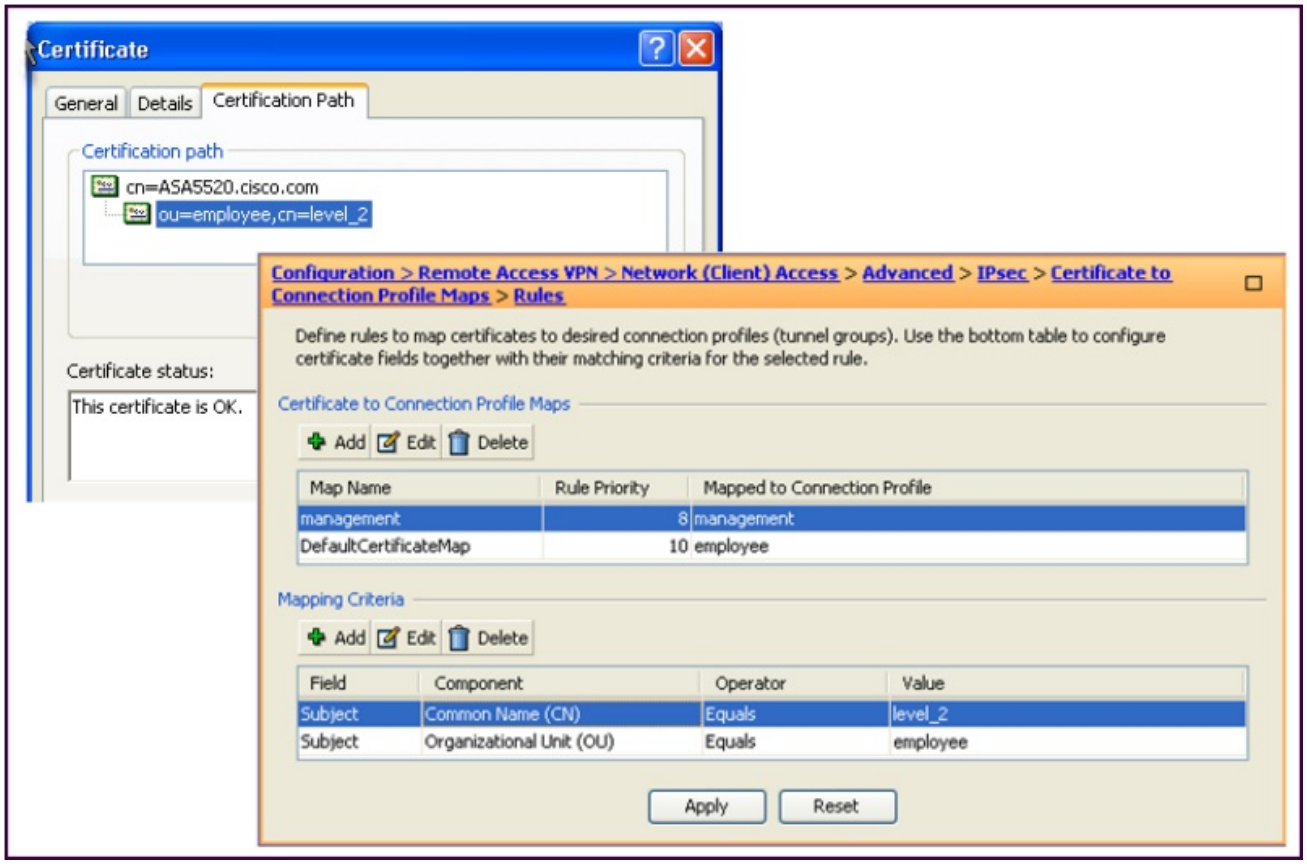
18. 展示を参照してください。

```
%ASA-5-713259: Group = contractor, Username = vpnuser, IP = 172.16.1.20, Session is being torn down. Reason: Phase 2 Mismatch
```

リモートアクセスアプリケーションのトラブルシューティングをしながら、新しい NOC エンジニアは、

展示に示されてロギングメッセージを受信しました。
どの構成が不一致である可能性が最も高いでしょうか?
A. IKE の設定
B. 拡張認証の設定
C. IPsec の設定
D. デジタル証明書の設定
Answer: C
Explanation:
http://www.cisco.com/en/US/tech/tk583/tk372/technologies_tech_note09186a00800949c5.shtmland %ASA-5-713259: Group = groupname, Username = username, IP = peerIP, セッションは切断されています。理由: ISAKMP セッション理由説明終了理由は、セッションがセッション管理によって取り壊されたときに発生し、これが表示されます。
グループ名セッションのトンネルグループが終了されている
ユーザ名、セッションのユーザ名が終了する
peerIP セッションのピアアドレスが終了する
理由はセッションの RADIUS 終了理由が終了されている。理由は、次のものがあり：
-ポートプリエンプト（同時ログイン）
-アイドルタイムアウト
-最大時間超過
-管理者のリセット

19. 展示を参照してください。



ABC 社は、事前共有鍵から証明書ベースの認証にリモートユーザ認証を変更している。ほとんどの社員

認証の場合は、そのグループメンバー（従業員）は、企業のアクセスを制御します。特定の管理担当者は、より機密性のサーバーにアクセスする必要があります。アクセスは、金融や LEVEL_2 としてグループと名前に基づいています。それはパイロットの時間新しい認証ポリシーである場合には、財務マネージャー、部門に割り当てられたサーバにアクセスすることができますが、制限されたサーバにアクセスすることはできません。
ネットワークエンジニアとして、どこに問題を探すでしょうか?
A. ファイナンスマネージャーの PC 上でのアイデンティティとルート証明書の妥当性をチェックします。
B. 接続プロファイルマップ>ルールの優先度 10 より大きい数にへの管理証明書を変更します。
C. 接続プロファイルマップ>規則に管理証明書が正しく設定されているかどうかをチェックします。
D. 接続プロファイルマップ>ポリシーの証明書が正しく設定されているか確認してください。
Answer: D
Explanation:
シスコ ASDM ユーザガイドバージョン 6.1

To configure the evaluation of IPSec or SSL VPN connections against certificate criteria-based rules, use the IPSec Certificate to Connection Maps > Rules or Certificate to SSL VPN Connections Profile Maps panel.

This panel lets you create the certificate-based criteria for each IPSec and SSL VPN connection profile, as follows:

Step 1 Use the table at the top (Certificate to Connection Profile Maps) to do one of the following:

- Create a list name, called a "map," specify the priority of the list, and assign the list to a connection profile.

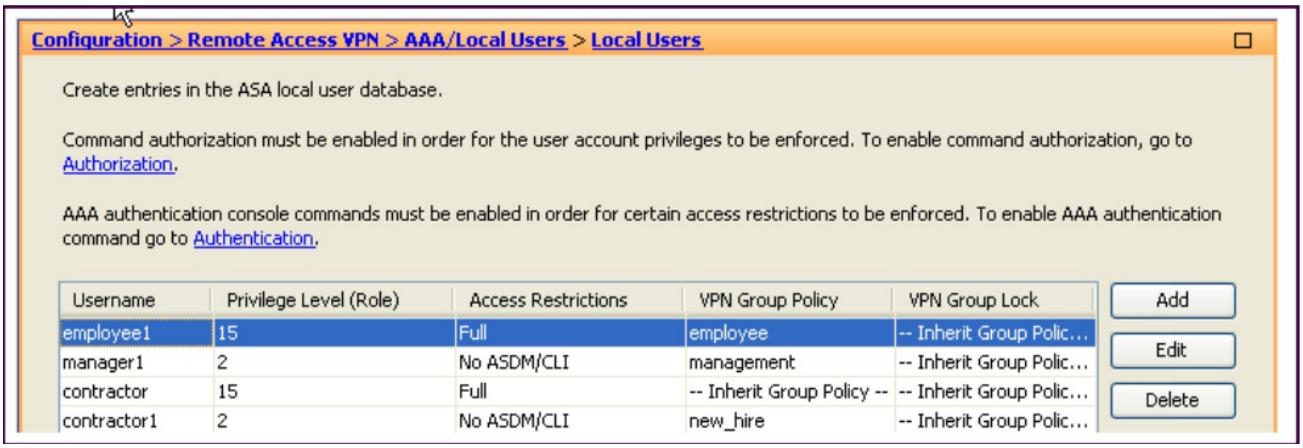
  ASDM highlights the list after you add it to the table.
- Confirm that a list is assigned to the connection profile for which you want to add certificate-based rules.

  ASDM highlights the list after you add it to the table and displays any associated list entries in the table at the bottom of the pane.

Step 2 Use the table at the bottom (Mapping Criteria) to view, add, change or delete entries to the selected list.

Each entry in the list consists of one certificate-based rule. All of the rules in the mapping criteria list need to match the contents of the certificate for the security appliance to choose the associated map index. To assign a connection if one criterion or another matches, create one list for each matching criterion.

20. 展示を参照してください。



VPN グループポリシーユーザーが"請負業者"継承ですか？

A. 従業員

B. 管理

C. DefaultWEBVPNGroup

D. DfltGrpPolicy

E. new_hire

Answer: D