2006 年 4 月（第 1 版）

Cisco Security Device Manager サンプル設定ガイド

SDM 2.1.2 2005/09 リリース版

Cisco Easy VPN サーバ

I 概　要

Cisco Easy VPN は、遠隔オフィスとテレワーカーのためのシンプルな仮想プライベート ネットワーク（VPN）構築を簡素化します。Cisco Easy VPN ソリューションは、すべての Cisco VPN デバイスの VPN 管理を集約し、VPN 構築における管理を容易にします。Cisco Easy VPN は、Cisco Easy VPN リモートと Cisco Easy VPN サーバの 2 つのコンポーネントから構成されています。

Cisco Easy VPN リモートの特徴は、遠隔地で必要となる作業ボリュームを最小にするよう、Cisco IOS ルータが Easy VPN サーバから受信する VPN トンネル接続に関するセキュリティポリシーを元に VPN を動的に構成する点です。このことは、遠く離れたオフィスに対して少ない IT サポートで費用対効果の高い理想的な解決策を提供することを意味していします。Cisco Easy VPN サーバは、サイト間接続またはリモートアクセス VPN ゲートウェイデバイスとして機能します。そこでは、リモートオフィス側のルータ（スポーク側）が Cisco Easy VPN リモートの機能を果たします。

このサーバクライアント機能は、主要サイトで定義されたセキュリティポリシーをリモート VPN 装置に配信し、それぞれの VPN 接続において、VPN の接続確立前に最適・最新のポリシーを適用することを確実なものとします。

Cisco Easy VPN サーバとして構成されたルータは、同様に Cisco Easy VPN リモートが有効になっているリモートルータからの VPN トンネルを終端することができます。Cisco Easy VPN リモートの大きな特徴は、内部 IP アドレス、内部サブネットマスク、DNS サーバアドレス、WINS サーバアドレス、スプリットトンネリングの有無などの VPN パラメータについて、リモートデバイスへ配信することです。本社などの中核サイトに保存された VPN 構成は、エンドユーザポリシーの動的な構成をサポートし、エンドユーザとフィールドエンジニアの作業工数を最小限にとどめます。これにより、設定ミスとそのために要するさらなるサポートコストを抑えることができます。このような特徴から、セキュリティポリシーの集中管理を提供する Cisco Easy VPN は、迅速なユーザ対応を必要とする大規模な VPN 展開において有効なソリューションとなります。

Cisco Easy VPN は、VPN トンネルに対する接続パラメータのネゴシエーションを行い、IP Security（IPSec）トンネルを確立するための自動管理を提供します。拡張認証（Xauth）は IPSec 接続を要求するユーザを特定するさらなる認証パターンを追加します。スプリットトンネリングは、インターネット向けのトラフィックについて、リモートルータがそれらのトラフィックを暗号化されたトンネルに送らず直接インターネットへ送信することを可能にする機能です。

II 設定手順

本設定ガイドでは以下の前提条件の下、LAN to LAN 接続での IPSec VPN 構成を想定しています。

(1) 固定 IP アドレスを持つ Cisco Easy VPN サーバ

(2) 固定または動的 IP を持つ Cisco Easy VPN リモート

(3) Cisco Easy VPN リモートは、Cisco Easy VPN サーバへ送信するトラフィックのみ暗号化

(4) リモート拠点（営業所）からのインターネット向けトラフィックは暗号化を行わず、直接送信される

(5) リモート拠点からのトラフィックはアドレス変換（NAT/PAT）が行われる

(6) ユーザレベルの認証は VPN アクセスの拡張認証によって行われる

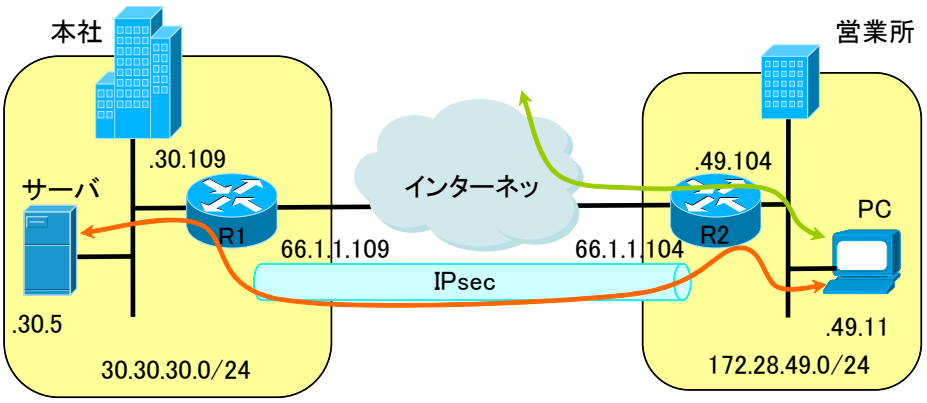


図 1：ネットワーク構成イメージ

本例では、事前共有キーは VPN 接続を行うルータを認証するのに使用し、拡張認証（Xauth）は IPSec 接続を要求するユーザを特定するための追加レベルの認証を提供します。リモートルータは、Internet Key Exchange（IKE）セキュリティ アソシエーションが確立された後に「ユーザ名/パスワード」チャレンジ認証を待ち受けます。

Cisco Easy VPN サーバ上でスプリットトンネリングが構成されている場合、このポリシーは Cisco Easy VPN リモートへ自動的に適用されます。スプリットトンネリングは、インターネット向けのトラフィックについてリモートルータが暗号化されたトンネルを通ることなく直接送信することを可能にしています。

本構成に使用する機器は、LAN および WAN インターフェイスが設定されており、SDM が利用できる状態にあるものとしています。

Cisco Easy VPN サーバ側では、認証、承認、および課金（AAA）サーバ、グループポリシー、および動的な暗号化マップの構成・設定を行います。以下のステップで Cisco SDM を使用した VPN 展開について説明します。

1. Cisco Easy VPN サーバの構成

Cisco Easy VPN サーバを構成するために、構成モードの VPN タスクを選択し、[Easy VPN サーバの作成]タグを選択します。画面中の[Easy VPN サーバの作成]をチェックし、「選択したタスクを実行する」をクリックして Easy VPN サーバウィザードを起動します(図 2)。

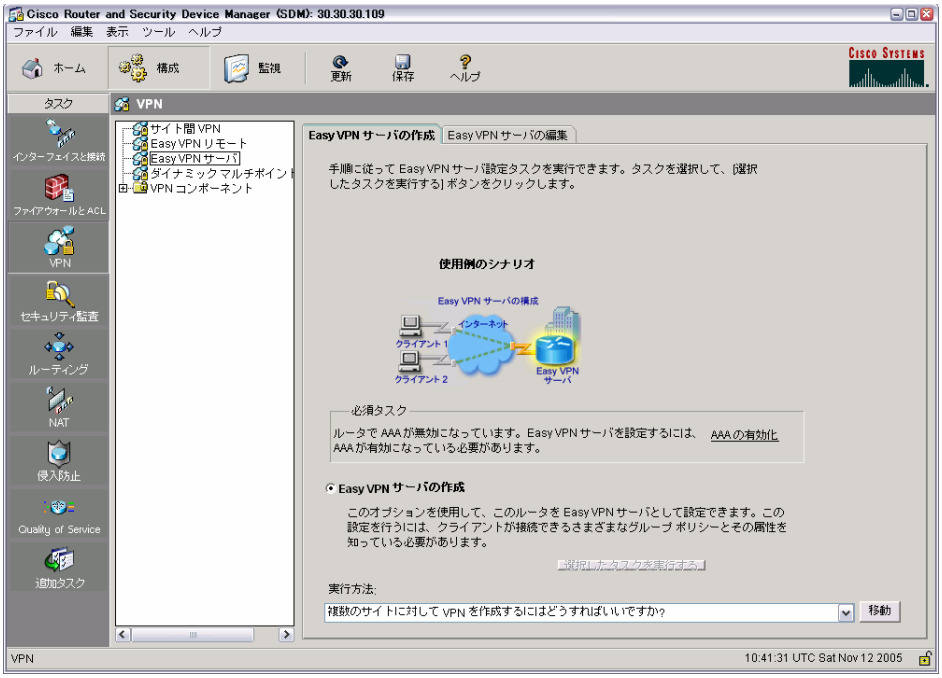


図 2:Easy VPN サーバの作成(AAA 未設定)

この例では AAA がまだ有効になっておらず、「選択したタスクを実行する」ボタンがグレーアウトして利用できなくなっています。AAA を有効にするには、「AAA の有効化」をクリックします。このとき、図 3/図 4 のメッセージが表示されます。図 3 の警告に示されるように、特権レベル 15 またはルートビューに関連付けられているユーザアカウントが存在しない場合、AAA 有効化後に SDM での接続ができなくなるので、AAA 有効化の前に特権レベル 15 またはルートビューに関連付けられたユーザアカウントを作成します。

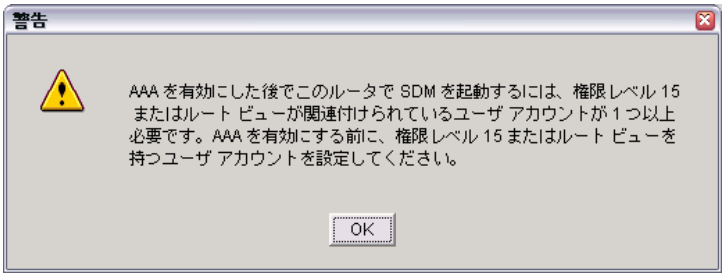


図 3:AAA 警告メッセージ

続いて、AAA 有効化処理は VTY 回線、コンソール回線、HTTP 認証についてルータのローカルユーザーデータベースを利用するようルータの設定を変更します。AAA を有効化するには「はい」をクリックします（図 4）。

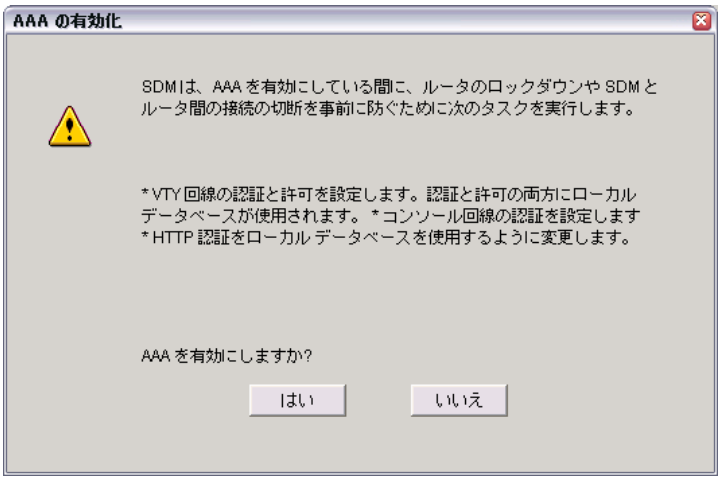


図 4：AAA の有効化

AAA の有効化が正常に行われると、図 5 のメッセージが表示されます。「OK」をクリックして処理を進めます。

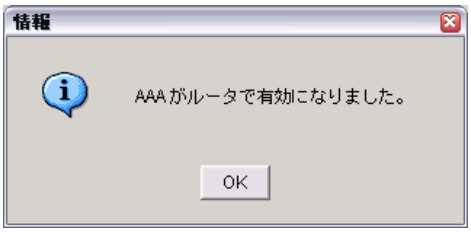


図 5：AAA の有効確認メッセージ

上記処理でルータの AAA を有効にした後、「選択したタスクを実行する」をクリックして Easy VPN サーバウィザードを起動します（図 6）。

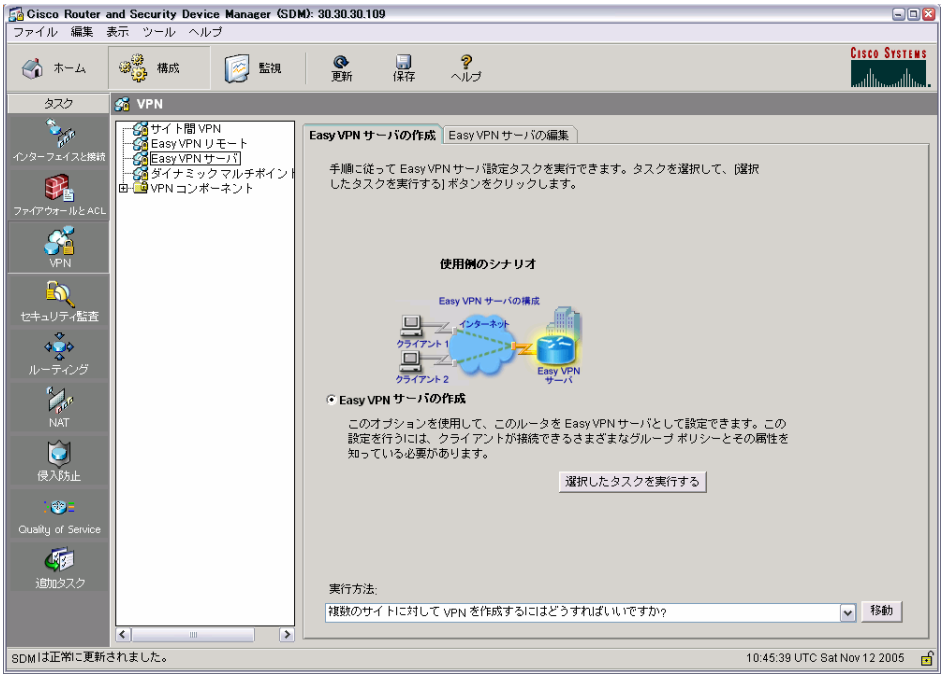


図 6：Easy VPN サーバの作成

Easy VPN サーバウィザード（図 7）が起動したら、画面に表示される情報に従って設定を進めます。「次へ」をクリックします。

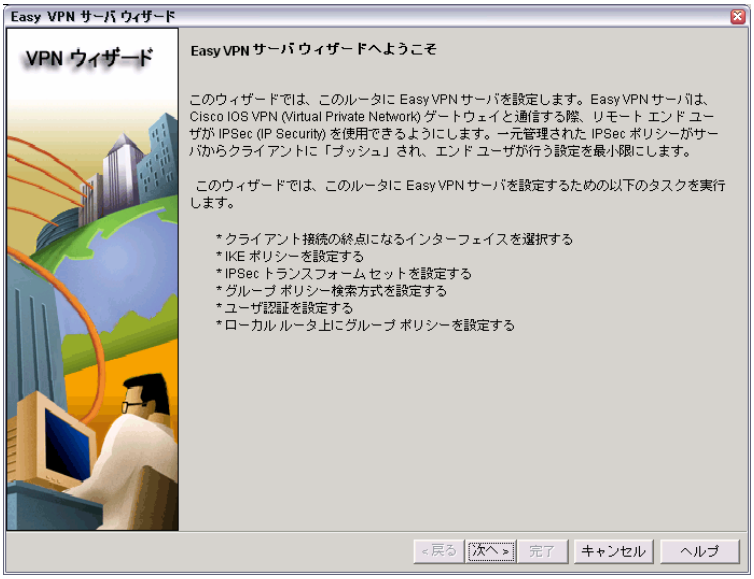


図 7：Easy VPN ウィザード

Easy VPN サーバに設定されている外部インターフェイスを指定します（図 8）。本例では FastEthernet1 を指定し、「次へ」をクリックします。

図 8：インターフェイスの指定

本例では、SDM のデフォルト IKE プロポーザルを使用します。「次へ」をクリックします（図 9）。

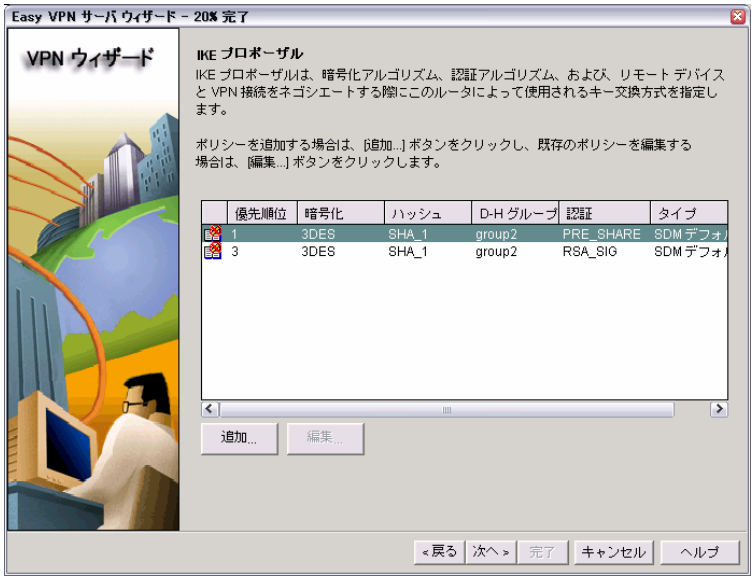


図 9：IKE プロポーザルの指定

本例では SDM デフォルトのトランスフォームセットを使用します。「次へ」をクリックします（図 10）。

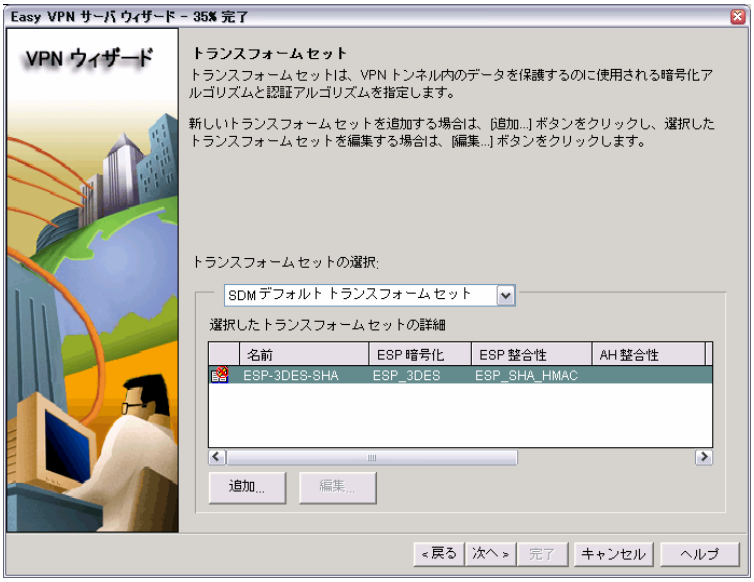


図 10：トランスフォームセットの指定

ISAKMP クライアントで認証情報などを共有するグループ認証/グループポリシーの参照先を指定します。本例ではルータ内のローカル情報のみを使用します。「ローカルのみ」をチェックし、「次へ」をクリックします（図 11）。

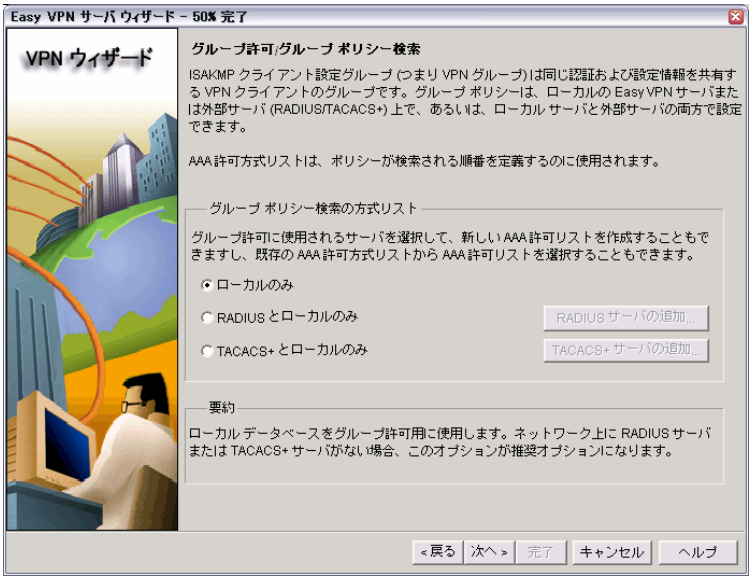


図 11：グループ認証設定

拡張認証の設定は次の手順で行います（図 12）。

①「ユーザー認証の有効化」をチェック

②「ローカルのみ」を選択

③「ユーザアカウントの追加」をクリックし新しいユーザアカウントを追加します。

図 12：拡張認証（Xauth）

ユーザアカウント画面（図 13）で「追加」をクリックすると、Cisco SDM からユーザ情報についての入力を求められます。

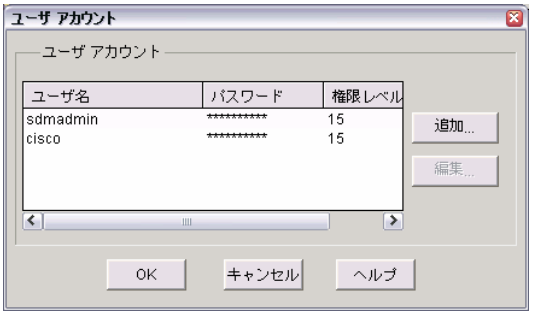
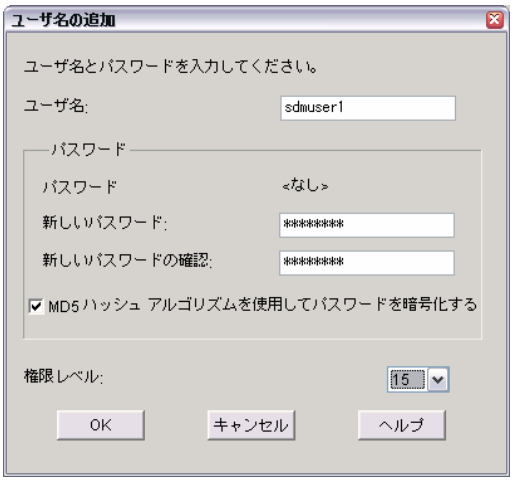


図 13：ユーザアカウント画面

ユーザ情報の入力として下記の内容を登録し、「OK」をクリックします（図 14）。



ユーザ名：sdmuser1

パスワード：cisco123（画面上は暗号化され表示されません）

MD5 によるパスワード暗号化：チェック

特権レベル： 15

図 14：ユーザ名の追加

新しいユーザアカウントが追加されたことを確認し、「OK」をクリックしてユーザアカウント画面を閉じます（図 15）。

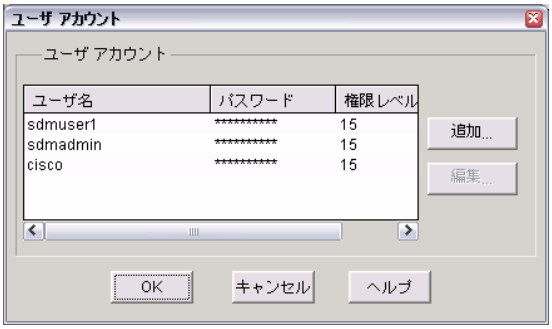


図 15：ユーザアカウントの確認

図 12 の画面に戻るので、そこで「次へ」を選びます。

グループ許可/ユーザグループポリシー画面で「追加」をクリックし、新しいポリシーを設定します（図 16）。

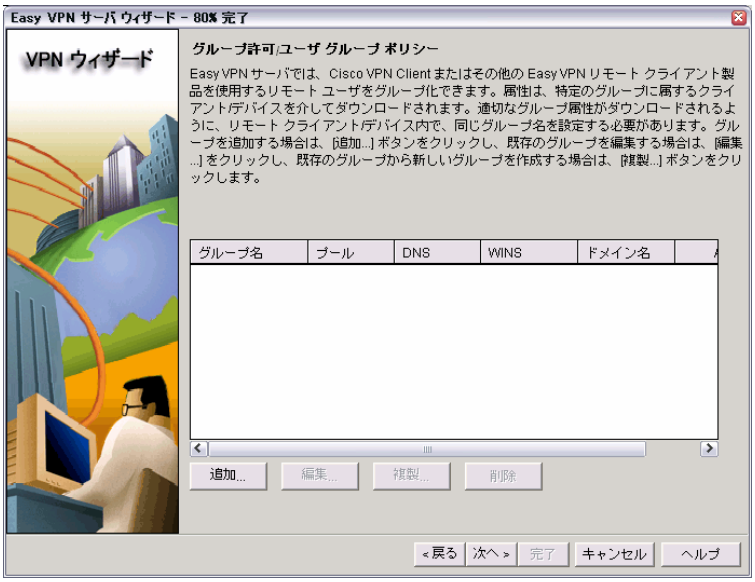
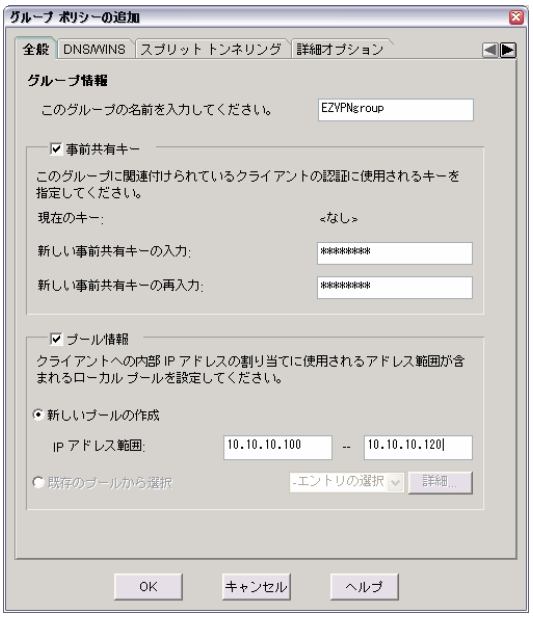


図 16：グループ許可/ユーザグループポリシー

グループポリシーの追加画面の［全般］タブで、以下の情報を入力します（図 17）。



グループ名：EZVPNgroup

事前共有キー：チェック

新しい事前共有キー：cisco123

プール情報：チェック

新しいプールの作成：チェック

IP アドレス範囲：10.10.10.100 ～ 10.10.10.120

図 17：グループポリシー（全般）

［DNS/WINS］タブを選択し、DNS 及び WINS サーバのアドレスを指定します。この例ではそれぞれプライマリが 30.30.30.5、セカンダリに 30.30.30.6 を入力し、ドメイン名には「cisco.com」を使用します（図 18）。

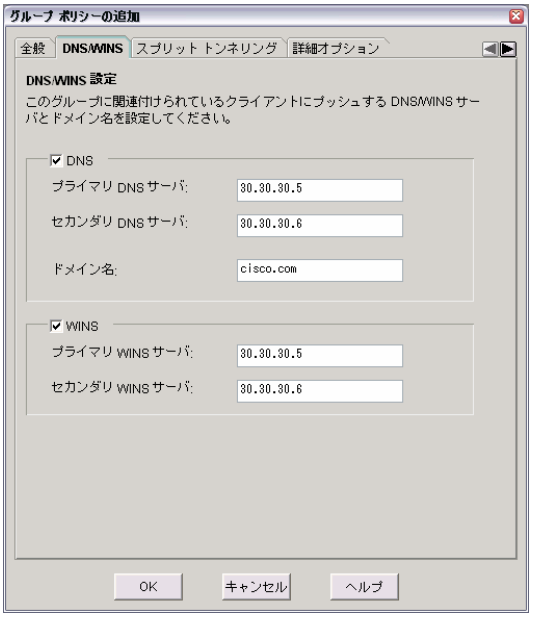


図 18：DNS/WINS 設定

［スプリットトンネリング］タブをクリックし、スプリットトンネリングを有効にします（図 19）。「追加」をクリックして保護されるネットワークである「30.30.30.0」（ワイルドカードビット 0.0.0.255）を入力します。

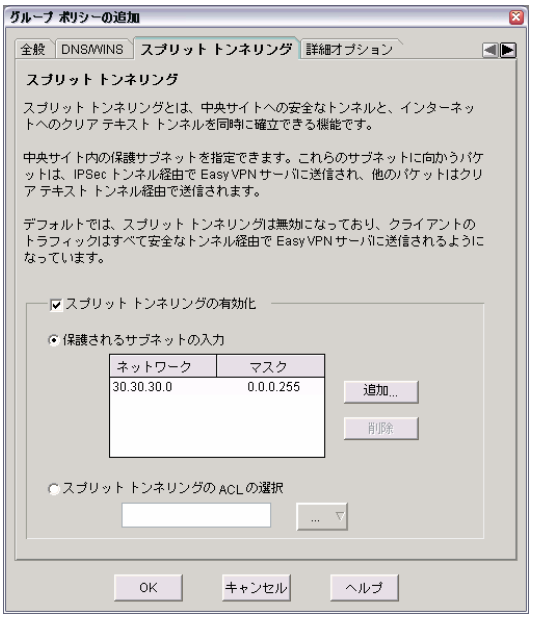


図 19：スプリットトンネリング

［XAuth オプション］タブを選択し、パスワードの保存をチェックします。また、ユーザあたりの最大ログイン数を 5 に設定し、「OK」をクリックします（図 20）

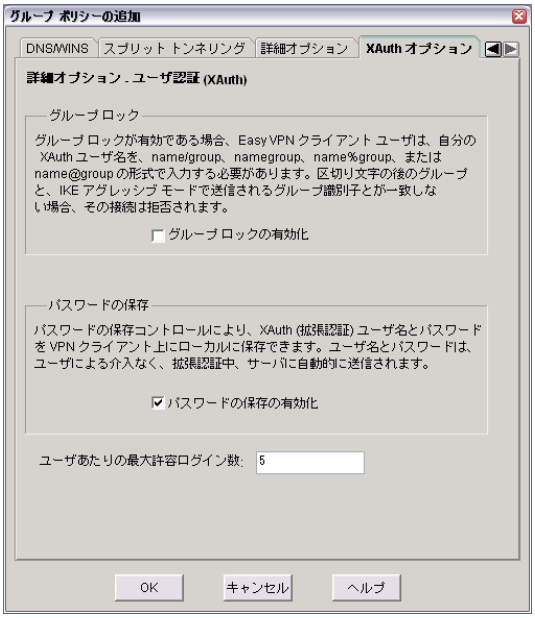


図 20：XAuth オプション

グループ許可/ユーザグループポリシーが新しく追加されたことを確認し、「次へ」をクリックします（図 21）。

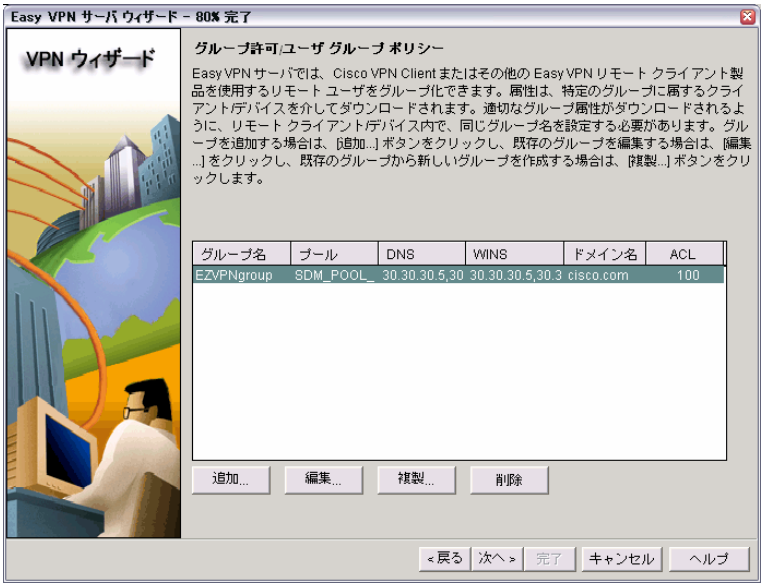


図 21：グループ許可/ユーザグループポリシーの確認

Easy VPN サーバに必要な設定は以上です。「完了」をクリックします（図 22）。

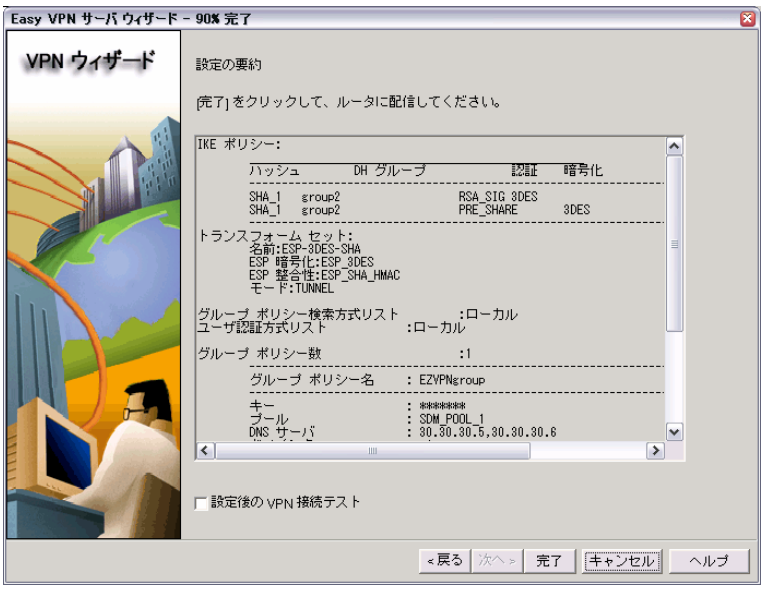


図 22：Easy VPN サーバ設定の確認

Easy VPN サーバウィザードが終了し、新しい Easy VPN サーバ設定が作成されました（図 23）。

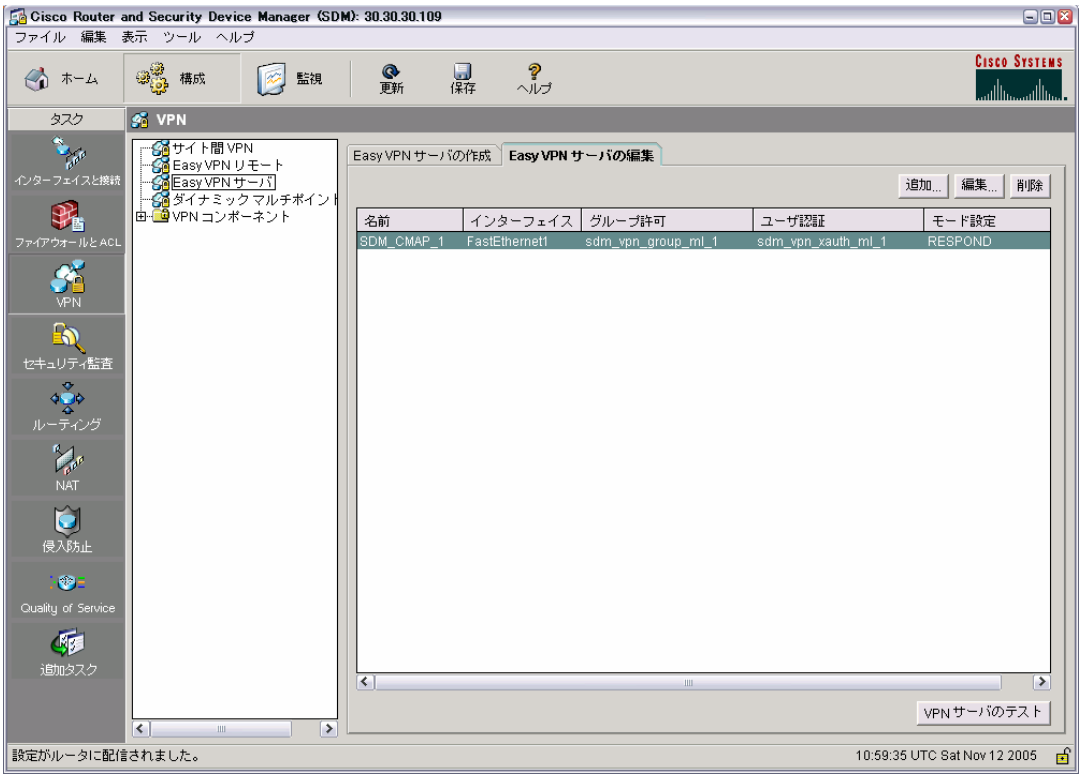


図 23：Easy VPN サーバ設定の完了

2. VPN 接続のモニタリング

Easy VPN サーバのステータスは、監視モードの VPN ステータスタスクから確認できます。[IPSec トンネルタブ]（図 24）では IPSec トンネルのトラフィック状況が、[Easy VPN サーバ]タブ（図 25）ではトラフィック状況に加えて Easy VPN サーバが払い出したプールアドレスの割り当てについても確認することができます。

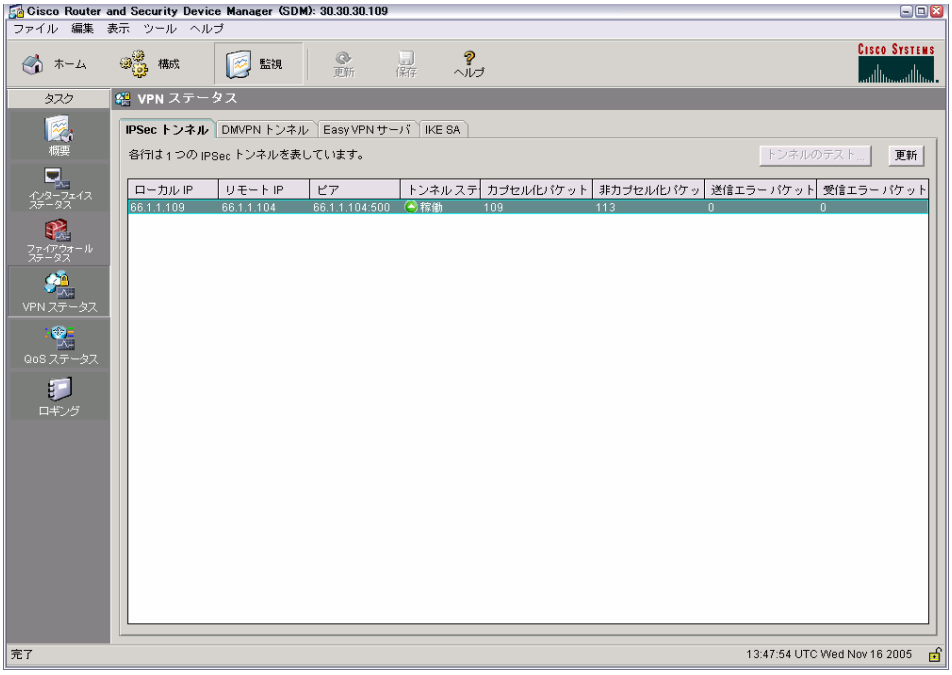


図 24：IPSec トンネルステータス

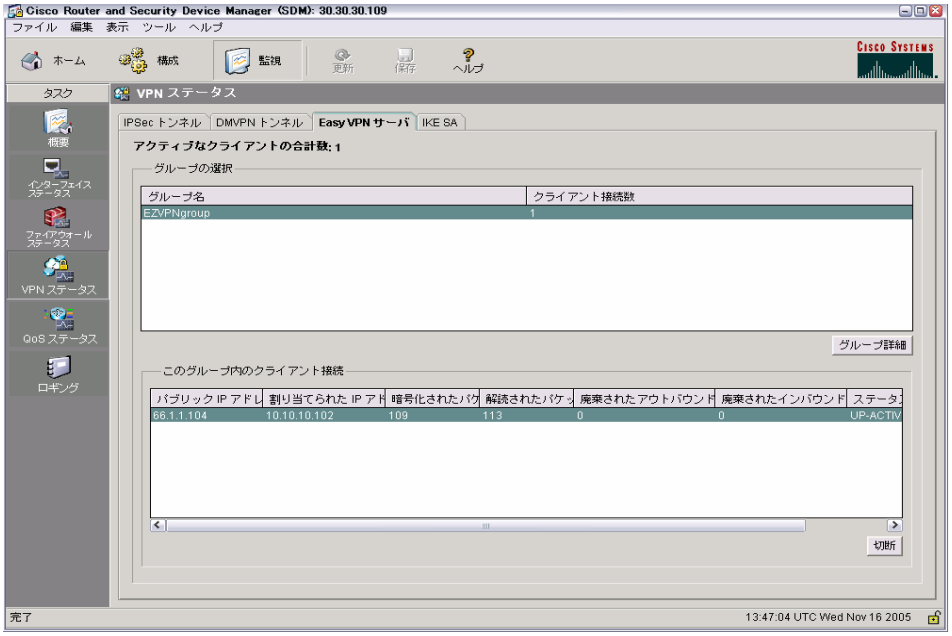


図 25：Easy VPN サーバステータス

参考:コマンドラインでの Easy VPN サーバ構成設定例

以下のコマンドラインインターフェイス(CLI)は、これまで SDM で行ってきたものと同様の構成を構築する際に使用するものです。

```
The Cisco Easy VPN Server Configuration
!
aaa new-model ! enable AAA
aaa authentication login ezvpnxauth local ! use local user database for Xauth
aaa authorization network ezvpnnetwork local ! use local user database for IKE queries
username sdmuser1 privilege 15 secret 0 cisco123 ! define local user database for Xauth
!
crypto isakmp policy 1 ! IKE Policy
authentication pre-share
encr 3des
hash sha
group 2
lifetime 86400
!
crypto isakmp policy 3
authentication rsa-sig
encr 3des
hash sah
group 2
lifetime 86400
crypto isakmp xauth timeout 60
!
ip local pool ezvpnpool 30.30.30.100 30.30.30.120 ! define local IP address pool
access-list 100 permit ip 30.30.30.0 0.0.0.255 any ! split tunneling access control list（ACL）
! Group policy pushed to Cisco Easy VPN Remote/Client
crypto isakmp client configuration group EZVPNgroup
key cisco123 ! define preshare key
pool ezvpnpool ! specify IP address pool
acl 100 ! split tunneling
dns 30.30.30.5 30.30.30.6
```

```
wins 30.30.30.7 30.30.30.8
domain cisco.com ! domain name for DNS
save-password ! Xauth: allow password save
max-logins 5
! Transform set
crypto ipsec transform-set my-transform esp-sha-hmac esp-3des
mode tunnel
!
crypto dynamic-map ezvpn-dymap 1 ! create a dynamic crypto map entry
set transform-set my-transform ! specify transform sets
set security-association lifetime seconds 3600
set security-association lifetime kilobytes 4608000
reverse-route ! set source proxy
!
crypto map MYCMAP 65535 ipsec-isakmp dynamic ezvpn-dymap ! add the dynamic map to a static map
!
crypto map MYCMAP isakmp authorization list ezvpnnetwork ! enable IKE queries
crypto map MYCMAP client authentication list ezvpnxauth ! enforce Xauth
crypto map MYCMAP client configuration address respond ! easy server responds to requests
!
interface FastEthernet0/1 ! apply the cryto map to the outside interface
crypto map MYCMAP
```

参考資料

Cisco Easy VPN Solution

http://www.cisco.com/en/US/partner/netsol/ns340/ns394/ns171/ns27/networking_solutions_sub_solution_home.html

Cisco Easy VPN White Paper

http://www.cisco.com/en/US/partner/netsol/ns340/ns394/ns171/ns27/networking_solutions_white_papers_list.html

Cisco Easy VPN Remote

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/ftezvpnr.pdf

1812J SDM config

```
!version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
no logging buffered
enable secret 5 $1$HkKz$nbBEh/L835LE3POv6LPqc1
!
aaa new-model
!
!
aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authorization exec default local
aaa authorization network sdm_vpn_group_ml_1 local
!
aaa session-id common
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
!
ip cef
```

```
no ip dhcp use vrf connected
!
!
no ip ips deny-action ips-interface
!
!
!
username cisco privilege 15 password 0 cisco
username sdmuser1 privilege 15 secret 5 $1$7aiw$jPeuahPNeI6qdFo6XZnTn.
!
!
!
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
!
crypto isakmp policy 3
 encr 3des
 group 2
!
crypto isakmp client configuration group EZVPNgroup
 key cisco123
 dns 30.30.30.5
 wins 30.30.30.5
 domain cisco.com
 pool SDM_POOL_1
 acl 100
 save-password
 max-logins 5
!
!
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
!
crypto dynamic-map SDM_DYNMAP_1 1
 set transform-set ESP-3DES-SHA
```

```
 reverse-route
!
!
crypto map SDM_CMAP_1 client authentication list sdm_vpn_xauth_ml_1
crypto map SDM_CMAP_1 isakmp authorization list sdm_vpn_group_ml_1
crypto map SDM_CMAP_1 client configuration address respond
crypto map SDM_CMAP_1 65535 ipsec-isakmp dynamic SDM_DYNMAP_1
!
!
!
interface BRI0
 no ip address
 shutdown
!
interface FastEthernet0
 ip address 30.30.30.109 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet1
 description $ETH-LAN$
 ip address 66.1.1.109 255.255.255.0
 duplex auto
 speed auto
 crypto map SDM_CMAP_1
!
interface FastEthernet2
!
interface FastEthernet3
!
interface FastEthernet4
!
interface FastEthernet5
!
interface FastEthernet6
!
```

```
interface FastEthernet7
!
interface FastEthernet8
!
interface FastEthernet9
!
interface Vlan1
 no ip address
!
ip local pool SDM_POOL_1 10.10.10.100 10.10.10.120
ip classless
ip route 10.10.10.0 255.255.255.0 FastEthernet1
!
!
ip http server
ip http authentication local
no ip http secure-server
!
access-list 100 remark SDM_ACL Category=4
access-list 100 permit ip 30.30.30.0 0.0.0.255 any
!
!
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
End
```

Cisco Security Device Manger サンプル設定ガイド
Cisco Easy VPN サーバ

発行　　2006 年 4 月　第 1 版

発行　　シスコシステムズ株式会社