ホワイトクラウド

ASPIRE

ホワイトクラウド ASPIRE

IPsec VPN 接続構成ガイド

ASA5515 を用いた接続構成例

ソフトバンク株式会社

注意事項

本資料内の記載は、飽くまでも情報提供のみを目的としております。明示、黙示、または法令に基づく想定に関わらず、これらの情報についてソフトバンク株式会社はいかなる責任も負わないものとします。本資料内に記載された社名・製品名は、各社の商標、または登録商標です。

更新履歴

版	更新日	更新者	更新内容
初版	2016/10/31	ソフトバンク株式会社	初版作成

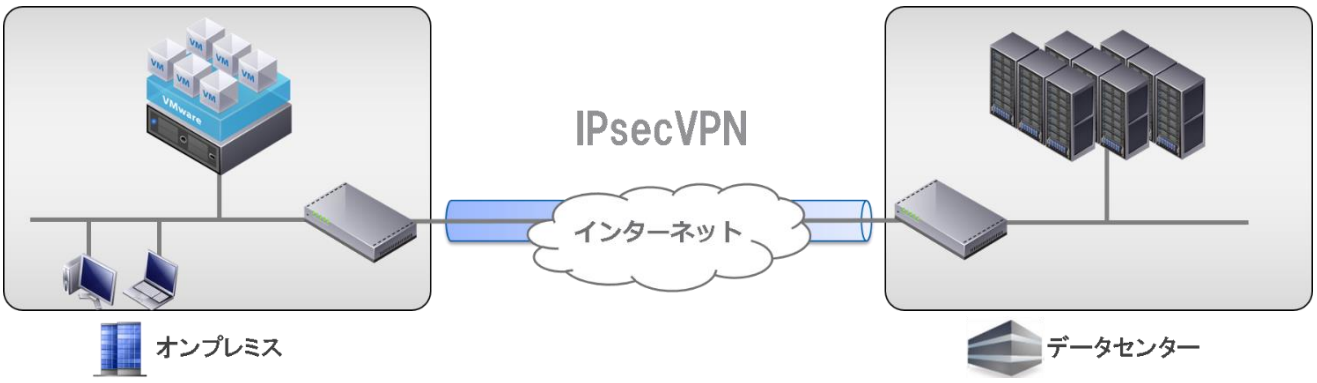
SoftBank

目次

1. ホワイトクラウド ASPIRE の IPsec VPN 機能概要

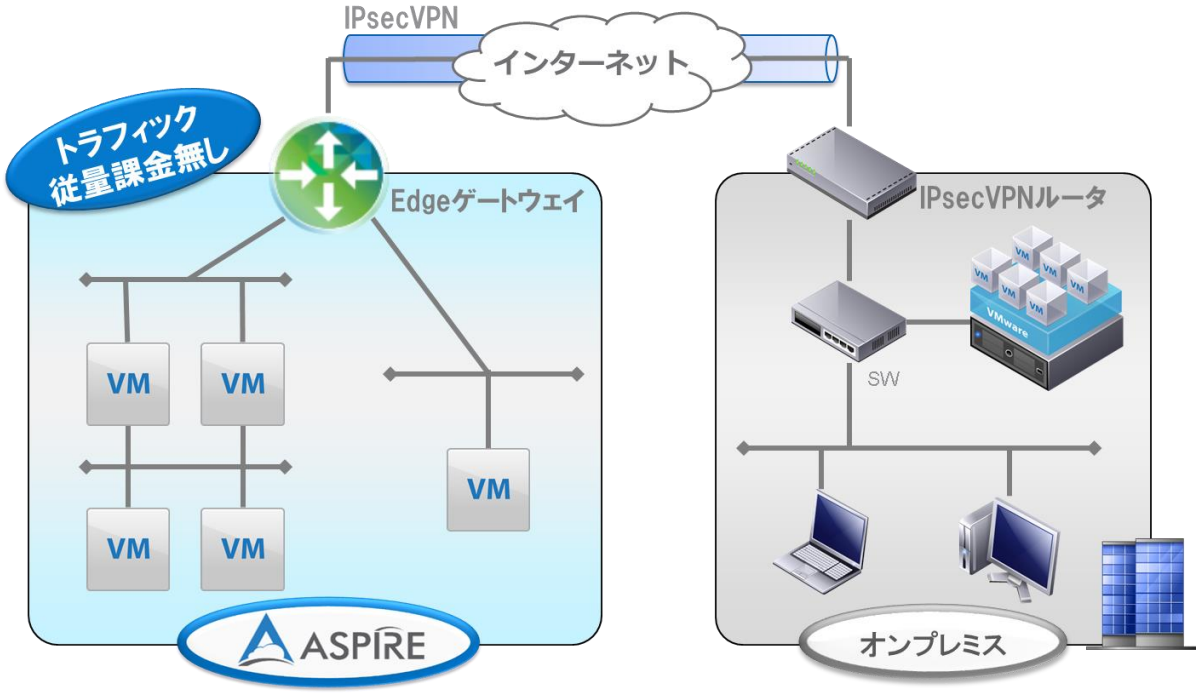
1.1. IPsec VPN について

IPsec (Security Architecture for Internet Protocol) は、IP 通信を暗号化することによって内容の秘匿と改ざん防止を実現するプロトコルです。この IPsec によって、異なる場所にあるネットワークやノードの間を、あたかも専用の回線を引いたかのように接続する技術が IPsec VPN です。この技術によって、重要性の高いデータ通信を安全に行うことができます。



1.2. ホワイトクラウド ASPIRE の IPsec VPN 機能

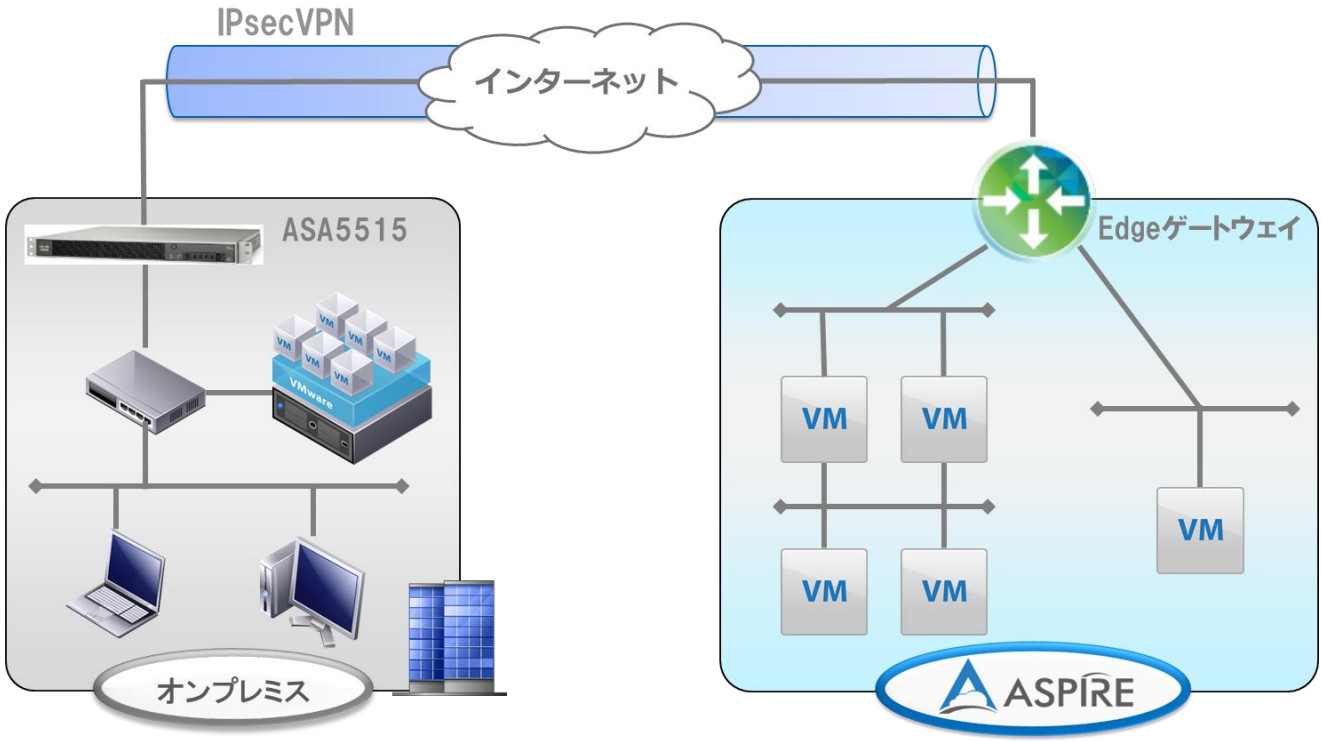
データセンタやオフィスなどの拠点との間で安全な通信を行うために、ホワイトクラウド ASPIRE は IPsec VPN 機能を標準搭載しています。ホワイトクラウド ASPIRE からインターネットへの接続に用いる Edge ゲートウェイが IPsec VPN 機能を提供します。IPsec VPN 接続機能を持つ拠点側の機器やソフトウェア等と Edge ゲートウェイの間で IPsec VPN による通信を行うことが可能です。



2. ASA5515 とホワイトクラウド ASPIRE の接続構成概要

2.1. 本資料でご紹介する ASA5515 を用いた構成

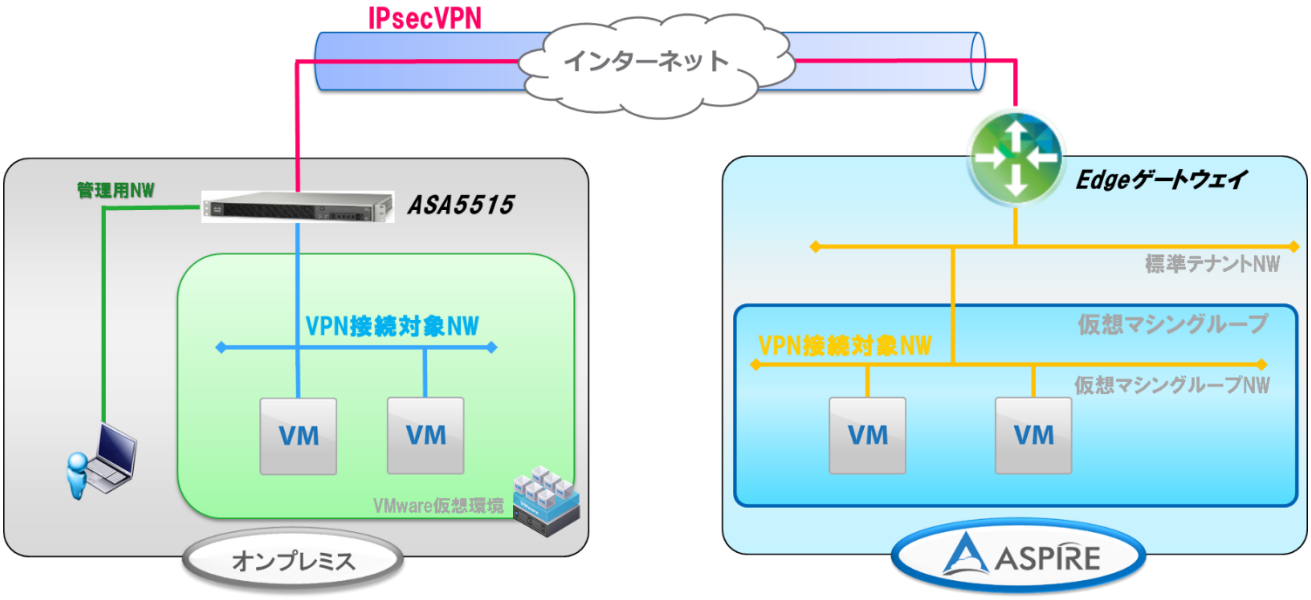
本資料では拠点側に ASA5515 を設置し、ホワイトクラウド ASPIRE の Edge ゲートウェイとの間を IPsec VPN で接続する設定例をご紹介します。



Cisco 製品の詳細に関しては、公式 Web サイトをご覧ください。
http://www.cisco.com/

2.2. 論理構成

オンプレミスとホワイトクラウド ASPIRE の VPN 接続対象ネットワーク間で通信できるように IPsec VPN を接続します。



次項より記載する構成手順は、上図のうち IPsec VPN 以外の部分が構成された状態を前提としております。本資料の作成にあたり使用した ASA 機器、OS バージョンは、下記となります。

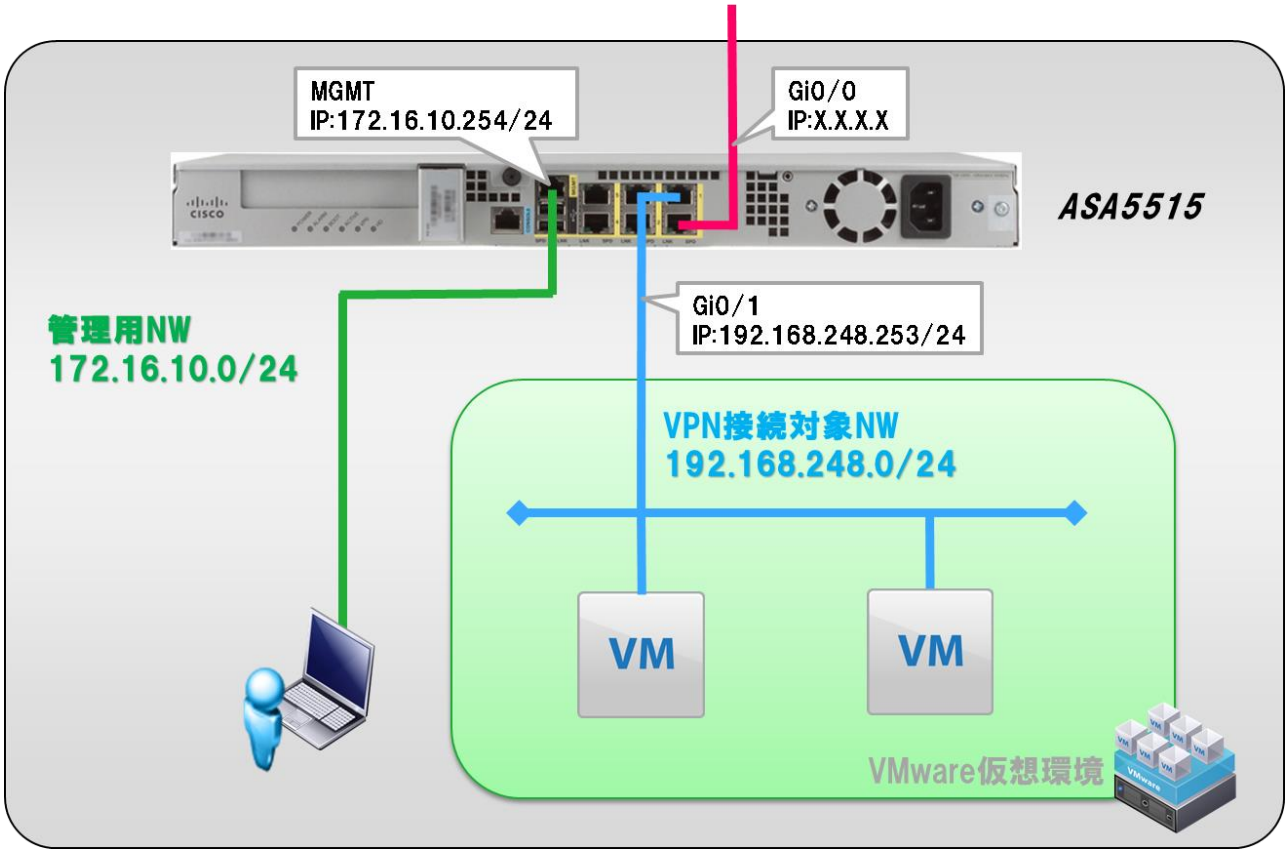
＜ ASA5515 ＞
機器:ASA5515
OS Version:9.2(3)4
ASDM Version:7.4(1)

3. 構成手順

3.1. 設定前の状態について

VPN 設定前のオンプレミスおよびホワイトクラウド ASPIRE それぞれの状態を示します。

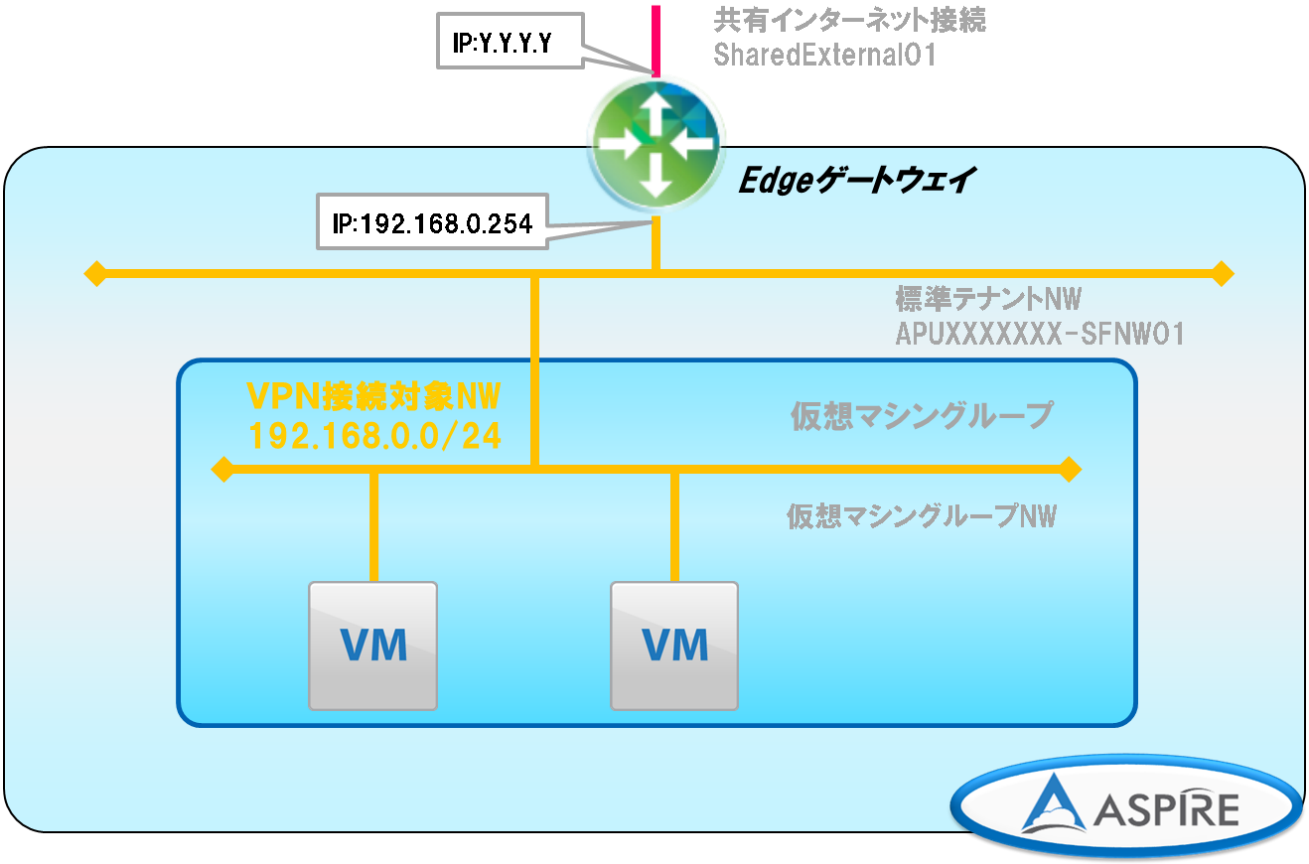
3.1.1. オンプレミス側 ASA5515 の設定



ASA5515

- ACL は WAN インターフェースへの設定のみ
- NAT は内→外のみ設定(NAPT)
- デフォルト GW は WAN 側に設定
- インターフェースは次の 3 つを使用
  - Gi 0/0（WAN）IP アドレス ：X.X.X.X
  - Gi 0/1（VPN 接続対象 NW）IP アドレス ： 192.168.248.253/24
  - Manage（管理用 NW）

3.1.2. ホワイトクラウド ASPIRE 側の設定



Edge ゲートウェイ

- ファイアウォールはルールの設定が無いものは全通信拒否
- NAT は内→外のみ（NAPT）
- VPN 接続対象 NW はデフォルトで存在する標準テナントNWを利用する
- インターフェースは次の2つを使用
  - Edge ゲートウェイ（WAN）IP アドレス：Y. Y. Y. Y
  - Edge ゲートウェイ（VPN 接続対象 NW）IP アドレス： 192.168.0.254/24

3.2. ASA5515 の VPN 設定

ASA5515 の VPN 設定手順を記します。大まかなステップは次のとおりです。

① ファイアウォール　オブジェクト設定
② IPsec VPN 設定
③ IPsec VPN 設定微調整

※前ページに記載された VPN 設定前の状態に至るまでの初期セットアップ手順は省略しております。
初期セットアップ手順はメーカー公開の各種ドキュメントをご参照ください。
http://www.cisco.com/web/JP/techdoc/index.html
※本資料では、Cisco ASDM を利用した設定方法を記載しております。CLI より設定される場合は、
巻末に参考 Config を記載しておりますのでそちらをご確認ください。

本資料で IPsec VPN の設定に利用する VPN パラメータを下記に示します。

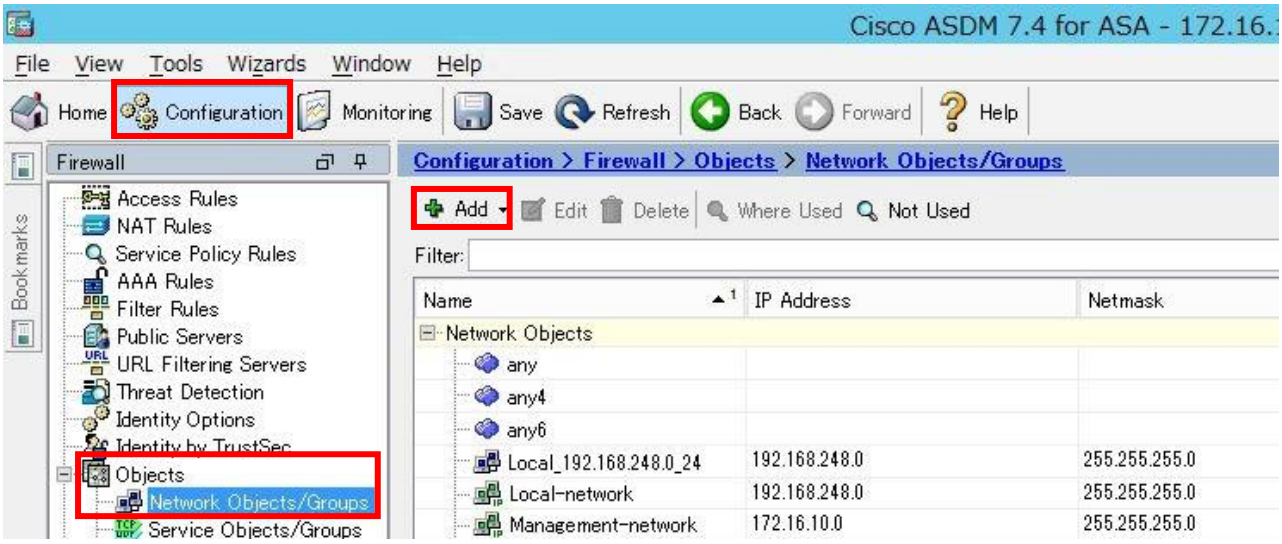
パラメータ	オンプレミス ASA5515	ホワイトクラウド　ASPIRE Edgeゲートウェイ
Local Network	192.168.248.0/24	192.168.0.0/24
Remote Network	192.168.0.0/24	192.168.248.0/24
Local ID	-	Y.Y.Y.Y
Remote ID	-	X.X.X.X
Remote IP	Y.Y.Y.Y	X.X.X.X
IKE version	V1	設定変更不可
認証方式	Pre-shared Key	設定変更不可
共有キー／Pre-shared Key	VpnaccessforASPIRE1vpnaccessforASPIRE1	VpnaccessforASPIRE1vpnaccessforASPIRE1
交換モード	Main mode	設定変更不可
暗号化・Hashアルゴリズム	AES256 / SHA-1	AES256 / SHA-1
Diffie-Hellman Group	group 2 (MODP1024 bits)	設定変更不可
PFS	On	設定変更不可
IKE SA Lifetime	28800 (no kbytes rekeying)	設定変更不可
IPsec SA Lifetime	3600 (no kbytes rekeying)	設定変更不可

※備考
・IKE フェーズ 1,2 では同じアルゴリズムを使用
・オンプレミス側の NW 機器でホワイトクラウド　ASPIRE の IPsec VPN 仕様に沿ったパラメータを設定する
・ホワイトクラウド ASPIRE 側は、ポリシーベース VPN のみ利用可能

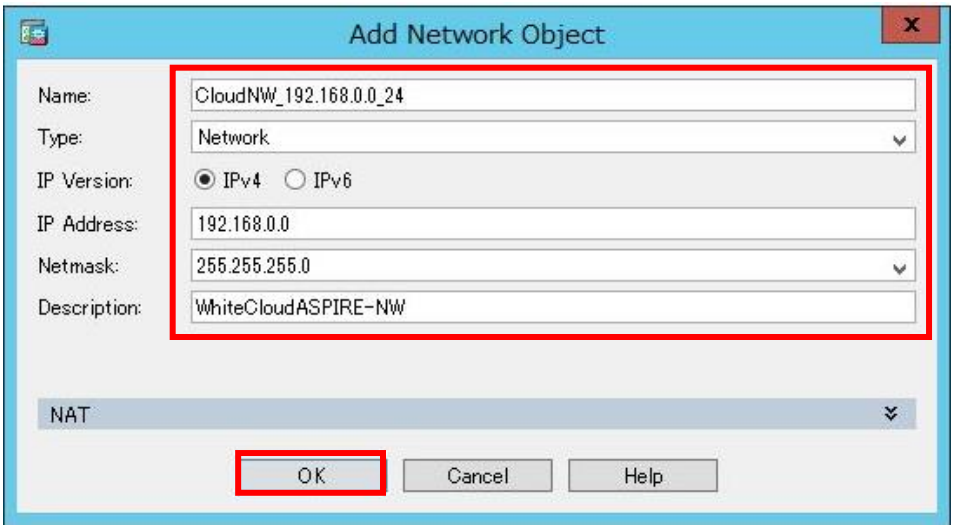
3.2.1. ファイアウォール　オブジェクト設定

Cisco ASDM より IPsec VPN の設定に利用するファイアウォールのオブジェクトを設定します。本資料ではローカル側のオブジェクトはすでに設定されています。ホワイトクラウド ASPIRE の VPN 対象ネットワークを オブジェクトとして登録します。

(1). メニューより「Configuration」→「Firewall」→「Objects」→「Network Objects/Groups」へアクセスし、「Add」をクリックします。



(2). ホワイトクラウド ASPIRE 上の VPN 対象ネットワークの情報を入力し「OK」をクリックします。

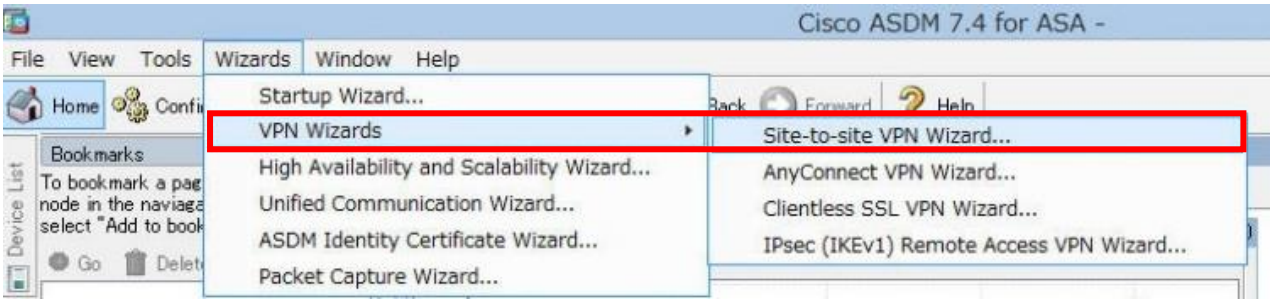


Name： 任意（本設定では CloudNW_192.168.0.0_24）
Type：Network を選択
IP Version：IPv4 を選択
IP address： ホワイトクラウド ASPIRE の VPN 接続対象 NW のセグメントを入力
Netmask： ホワイトクラウド ASPIRE の VPN 接続対象 NW のサブネットマスクを選択
Description： 任意

3.2.2. IPsec VPN 設定

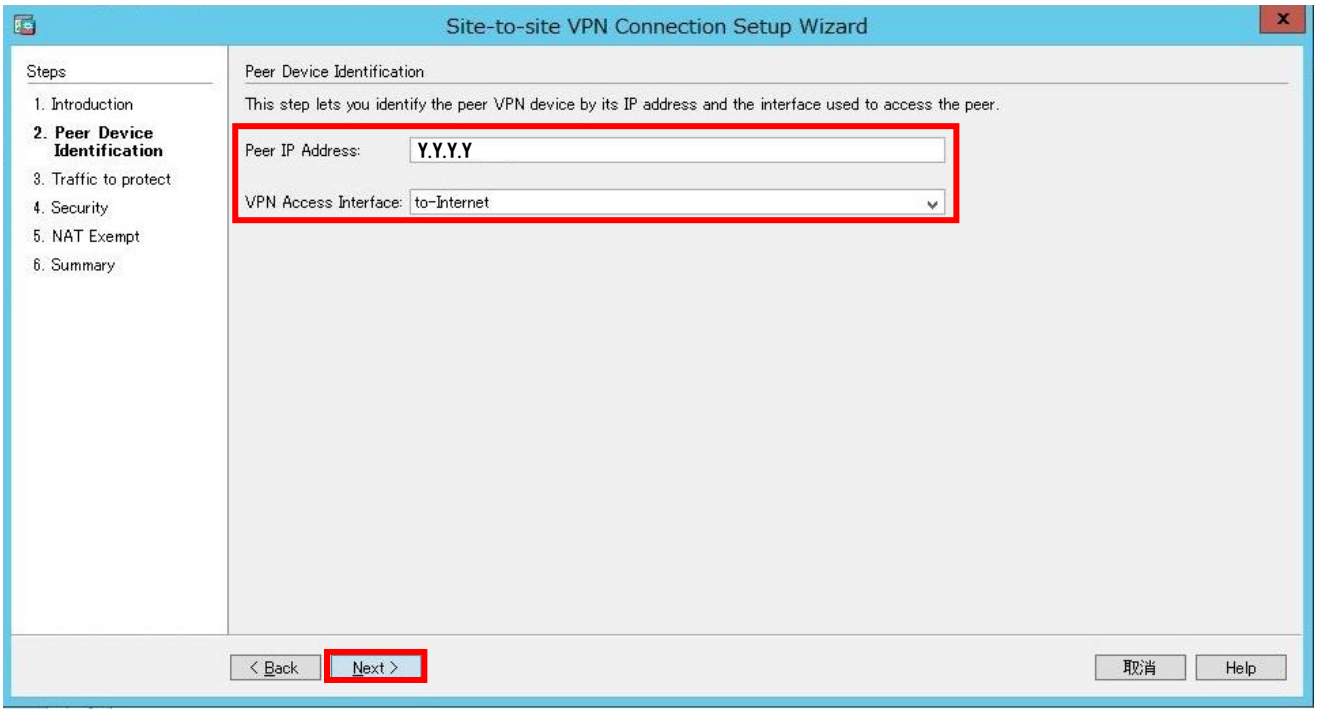
IPsec VPN を利用する対象ネットワーク、暗号アルゴリズム等の各パラメータを設定します。
Cisco ASDM のウィザードを用いて IPsec VPN を設定します。

(1). メニューより「Wizards」へアクセスし「VPN Wizards」→「Site-to-site VPN Wizard」をクリックします。



(2). 「Next」をクリックします。

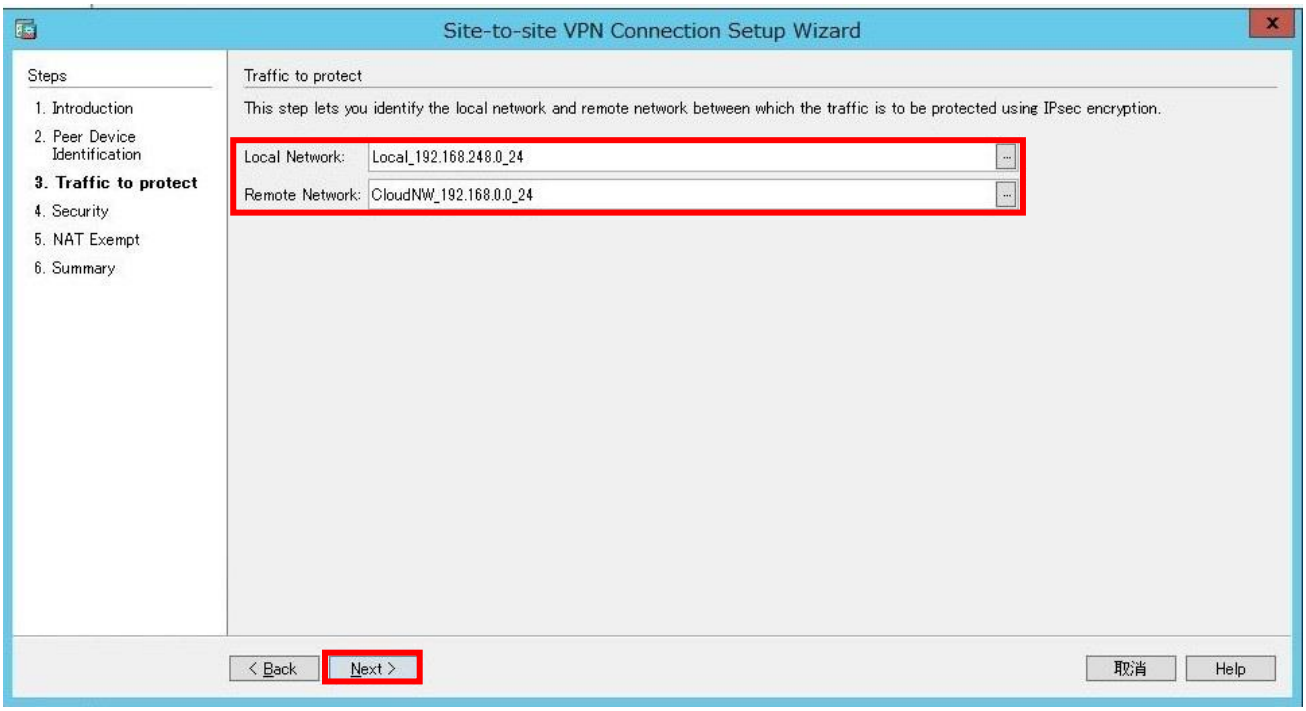
(3). VPN 接続先の情報を入力し「Next」をクリックします。



Peer IP Address ： ホワイトクラウド ASPIRE の Edge ゲートウェイのグローバル IP アドレスを入力

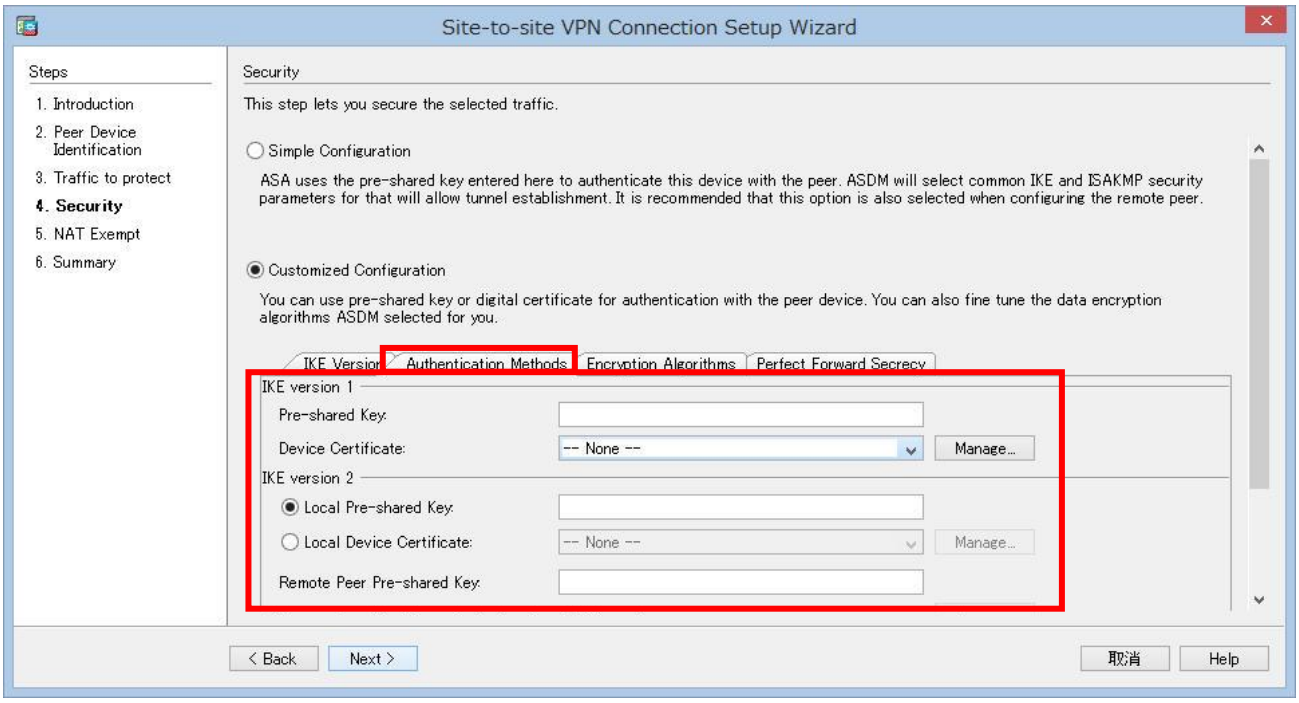
VPN Access Interface ： ASA5515 の WAN 側インターフェースを選択

(4). VPN 接続対象 NW を設定し「Next」をクリックします。



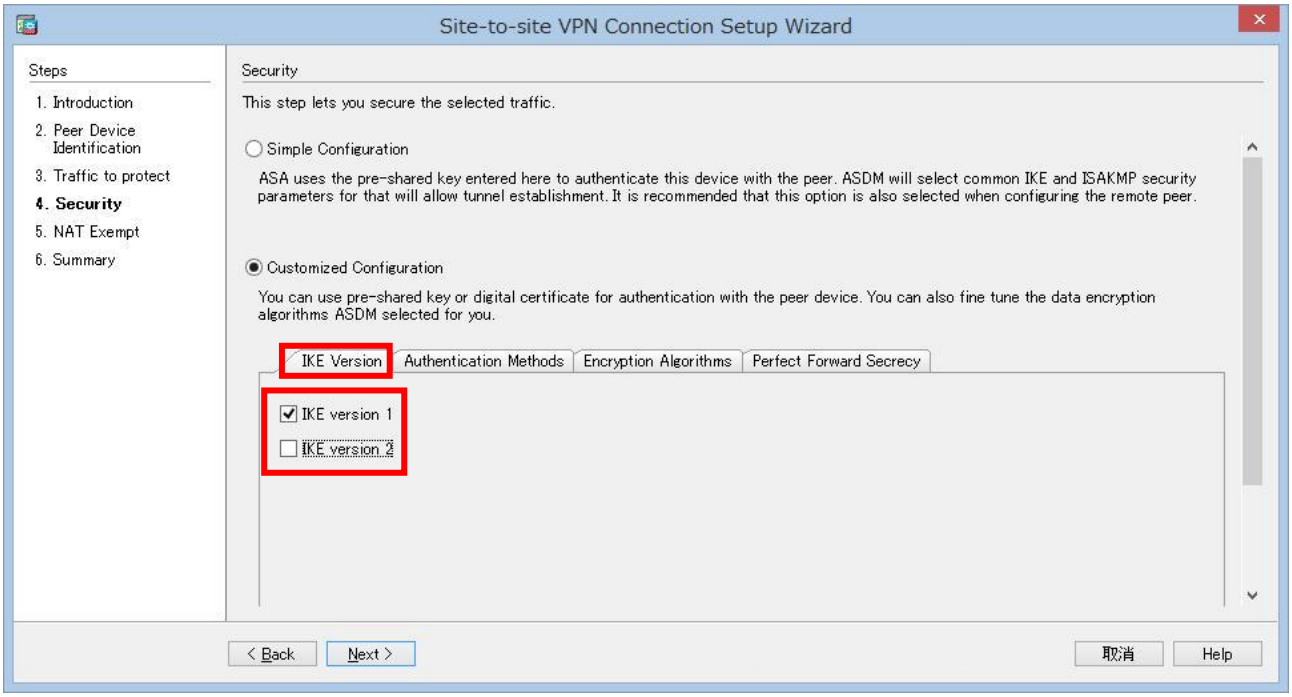
Local Network：オンプレミスの VPN 接続対象 NW を選択（本設定では Local_192.168.0.0_24）
Remote Network：ホワイトクラウド ASPIRE の VPN 接続対象 NW を選択
（本設定では CloudNW_192.168.0.0_24）

(5)．セキュリティ(暗号化方式)を設定します。

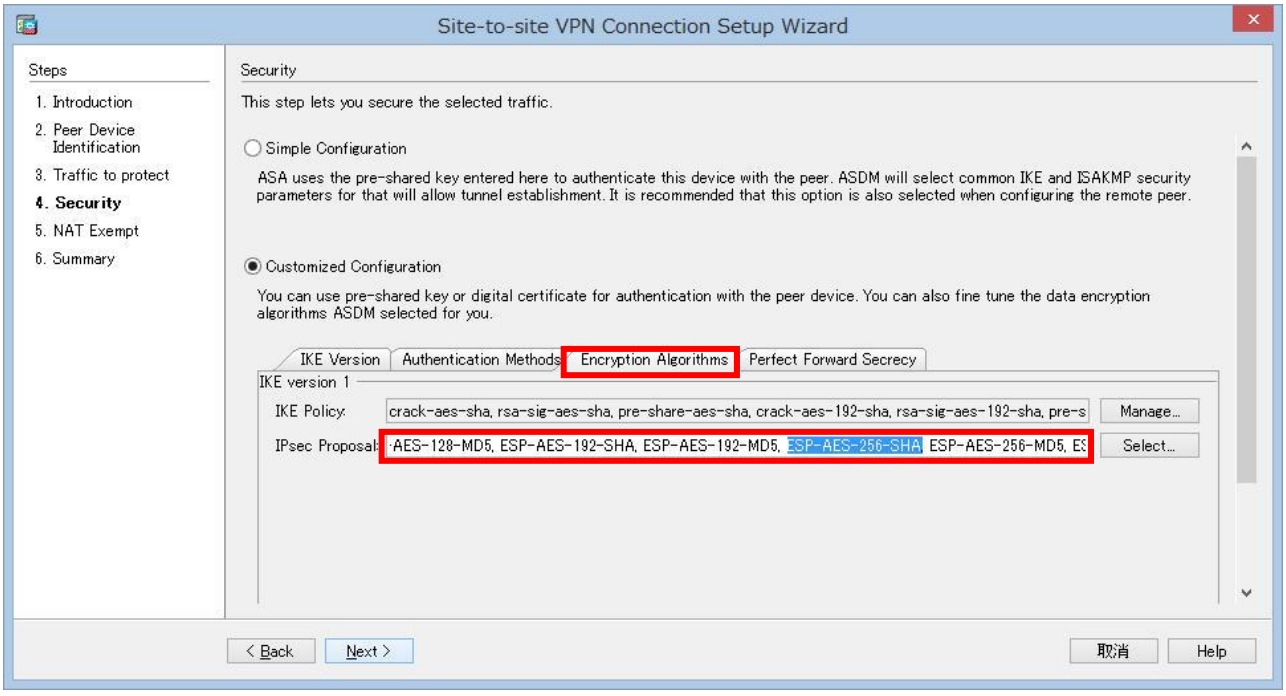


Customoized Configration ： 有効
IKE version1 Pre-shared Key ： 共有キーを入力
IKE version2 Pre-shared Key ： 共有キーを入力
※Pre-Shared Key(共有シークレット)は、32 ～ 128 文字の範囲内の英数字で指定し少なくとも 1 つの大文字、1 つの小文字、および 1 つの数字を含んでいなければなりません。
(本設定では vpnaccessforASPIRE1vpnaccessforASPIRE1)
※ホワイトクラウド ASPIRE では IKE version2 は利用できません。ASA5515 の Setup Wizard の仕様上、IKE version2 の Pre-shared Key を入力しないと他の設定タブへ画面遷移ができません。

(6).「IKE version」タブをクリックします。「IKE version2」のチェックを外します。



(7).「Encription Algorithms」タブを選択し利用する暗号化方式が含まれていることを確認します。

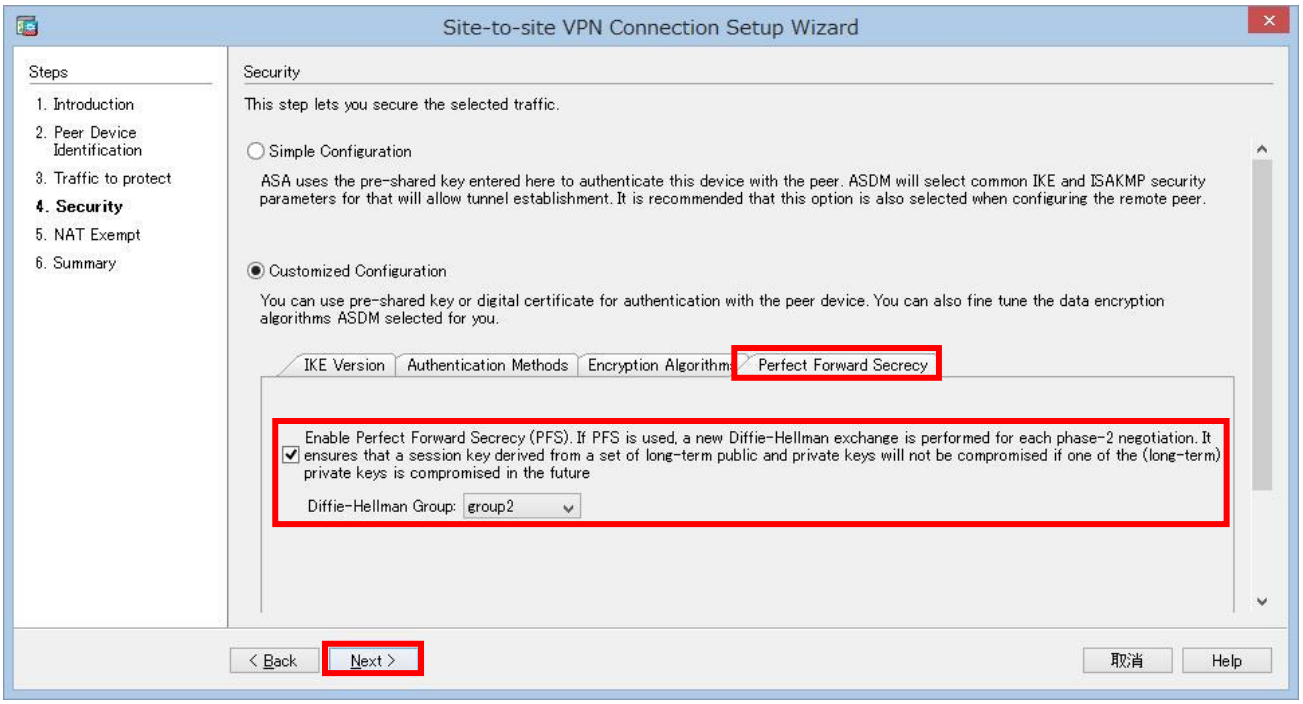


本設定では下記を利用します。

IKE Policy ： pre-share-aes-256-sha

IPsec Proposal ： ESP-AES-256-SHA

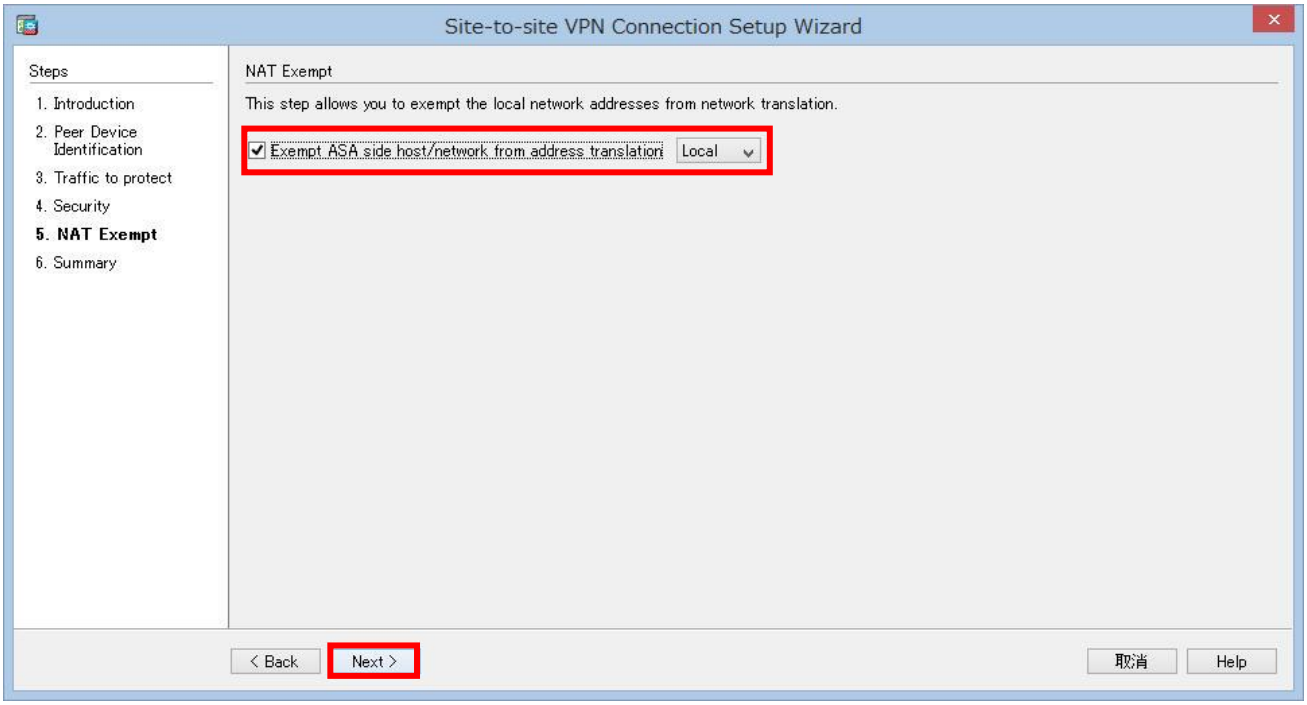
(8). 「Perfect Forward Security」 を設定し、「Next」 をクリックします。



Enable Perfect Foard Security ： 有効

Diffie-Hellman Group ： Group2

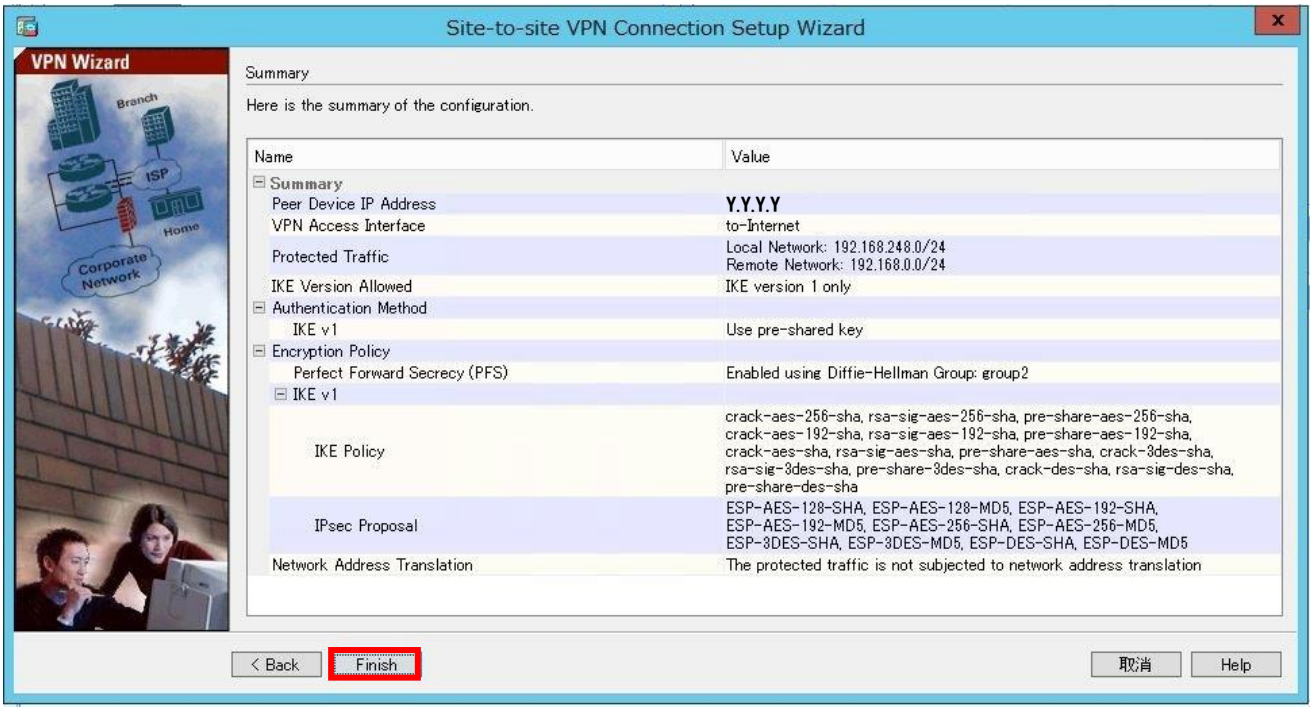
(9). NAT Exempt を設定し、「Next」 をクリックします。



Export ASA Side host/network from address translation ： 有効

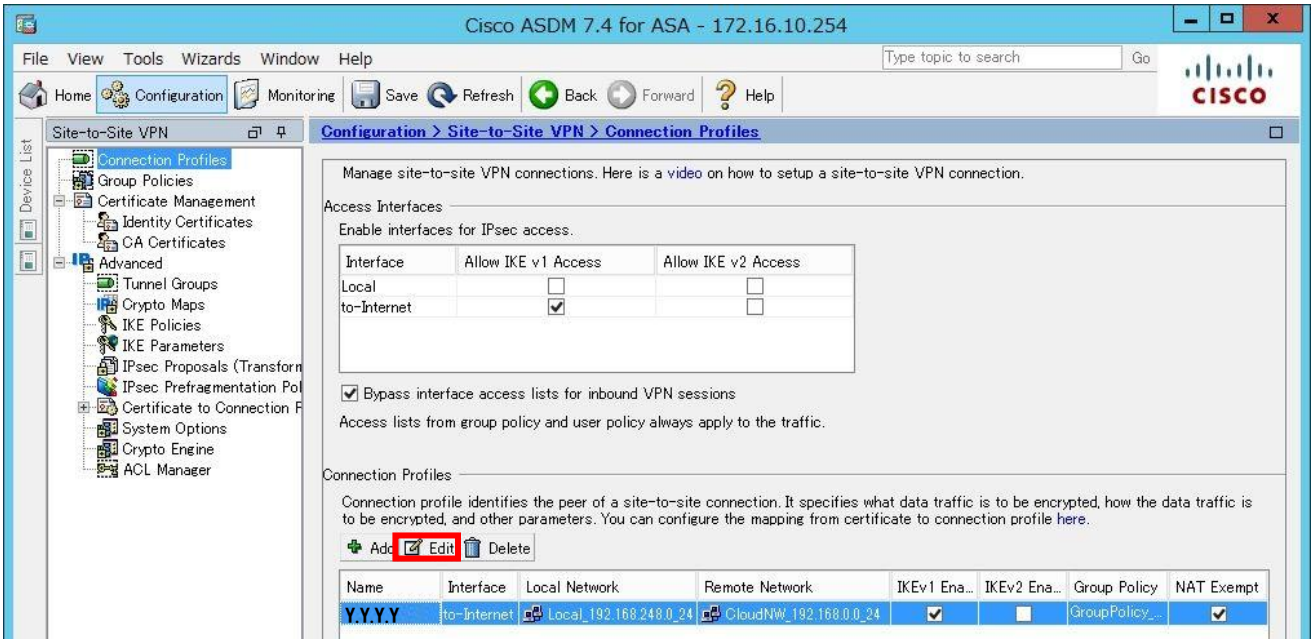
NAT から除外するホストまたはネットワークを選択 （本設定では Local）

(10). 設定内容を確認し「Finish」をクリックします。

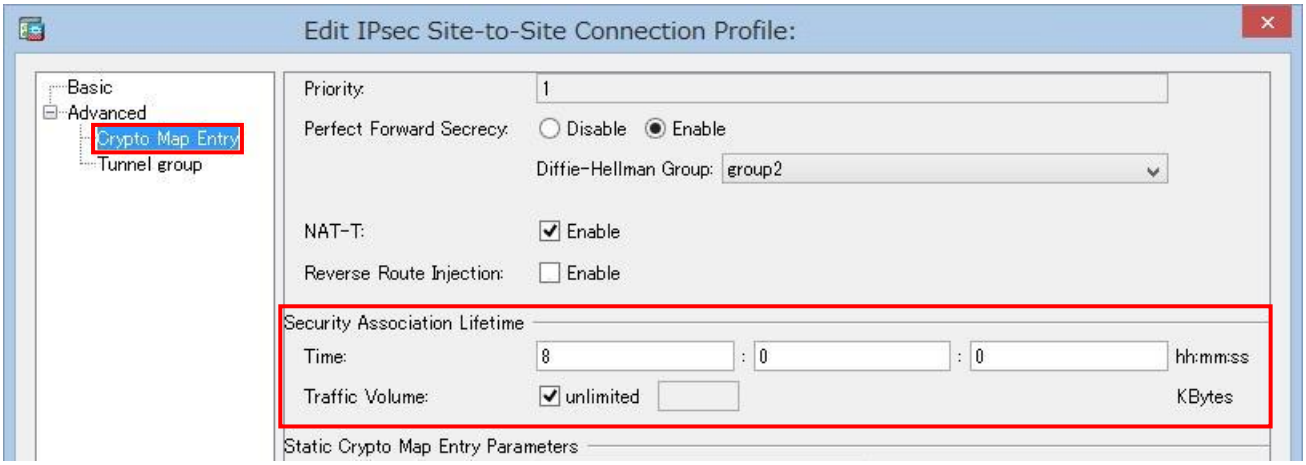


3.2.3. IPsec VPN 設定微調整

(1). VPN 設定の微調整を行います。「Edit」をクリックします。



(2).「Crypto Map Entry」の「Security Association Lifetime」の設定を修正します。

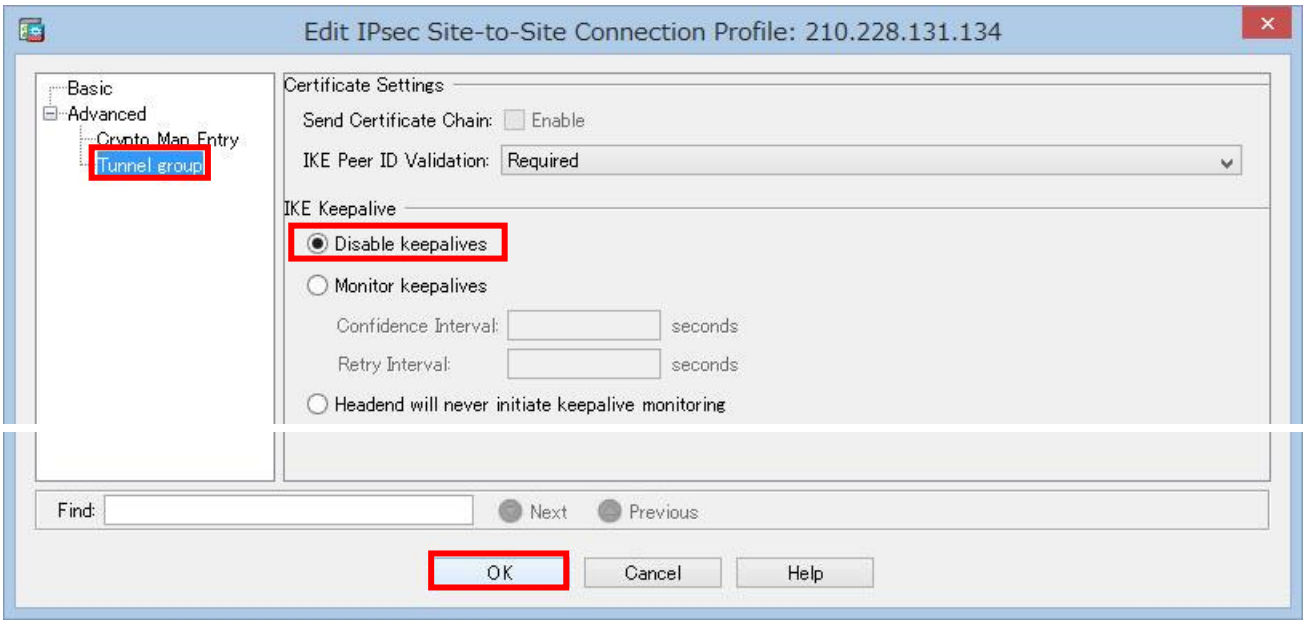


Time ： 8:00:00

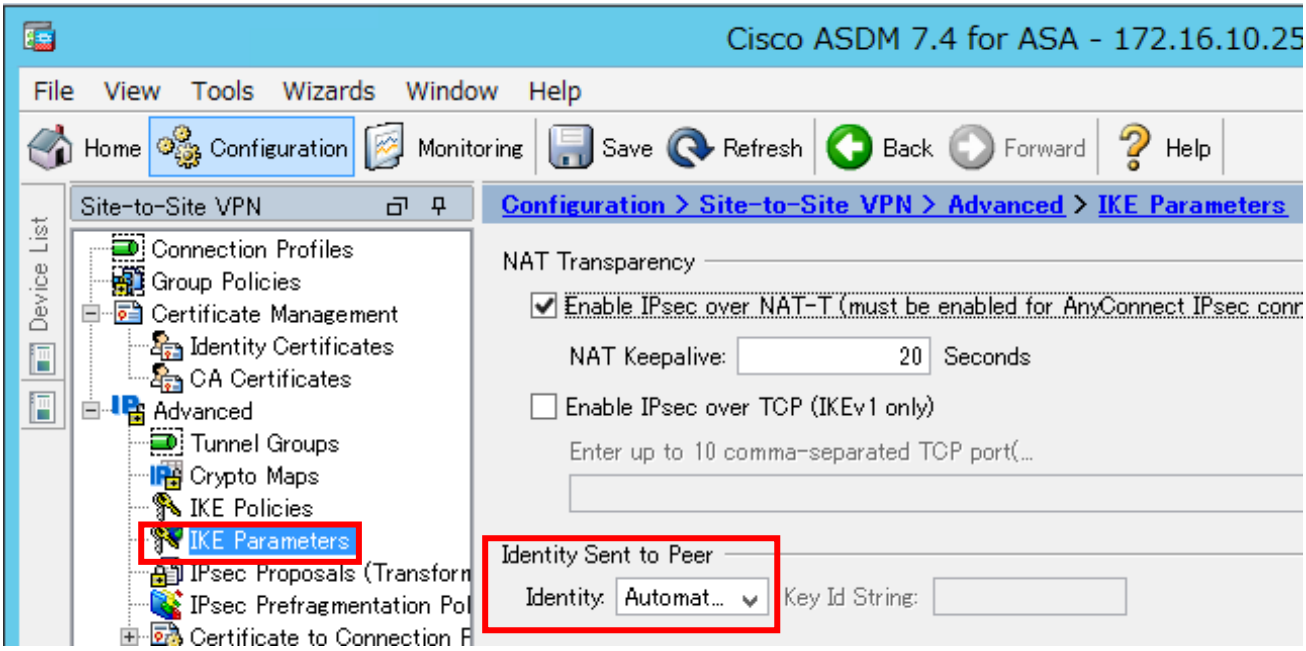
Traffic Volume ： unlimited

(3).「Tunnel group」の「IKE Keepalives」の設定を修正します。

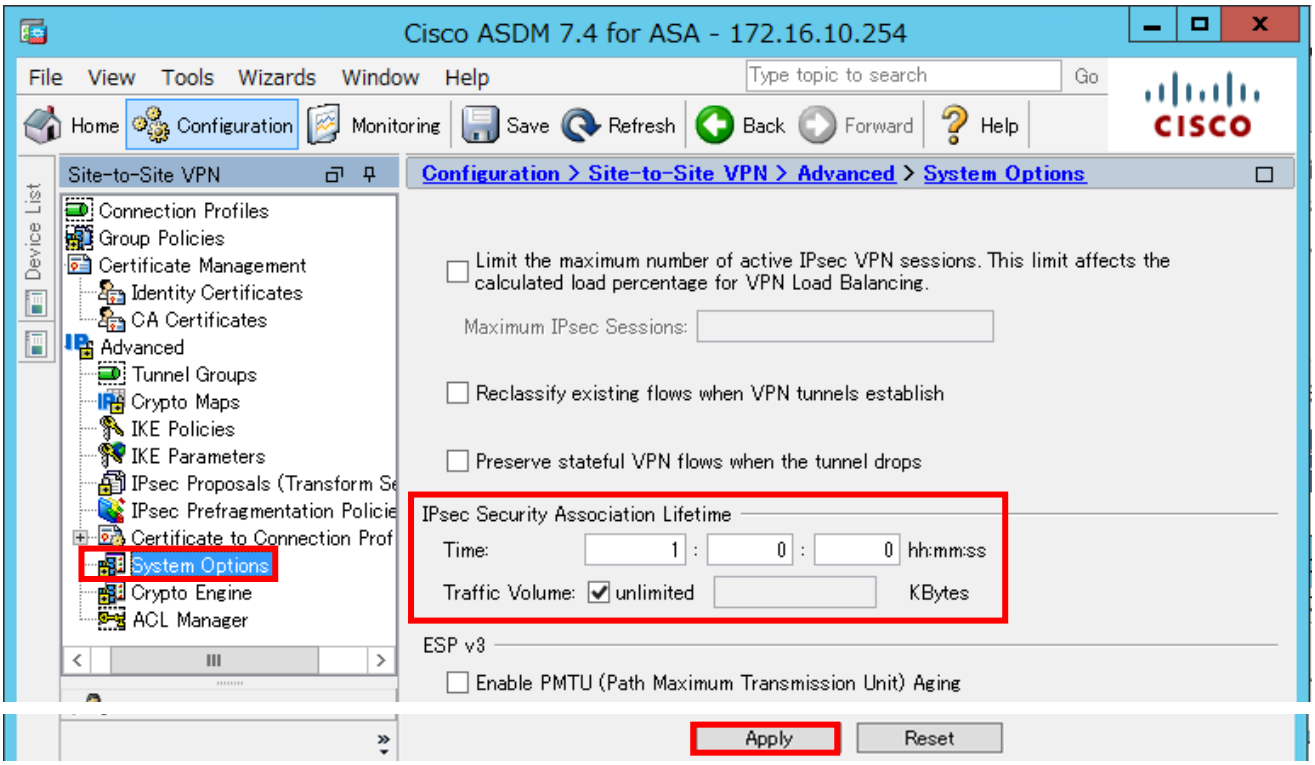
「Disable keepalives」を選択し、「OK」をクリックします。



(4).「Site-to-Site VPN」の「IKE Paramater」の設定を修正します。
メニューより「Configuration」→「Site-to-Site VPN」→「Advanced」→「IKE Paramater」へアクセスします。「Identity Sent to Peer」の「Identity:」を「Automatic」もしくは「Address」へ変更します。



(5).「System Options」の「IPsec Security Association Lifetime」を修正し「Apply」をクリックします。



Time ： 1:00:00
Traffic Volume ： unlimited

3.3. ホワイトクラウド ASPIRE の VPN 設定

ホワイトクラウド ASPIRE とオンプレミスの ASA5515 を IPsec VPN で接続する設定を行います。

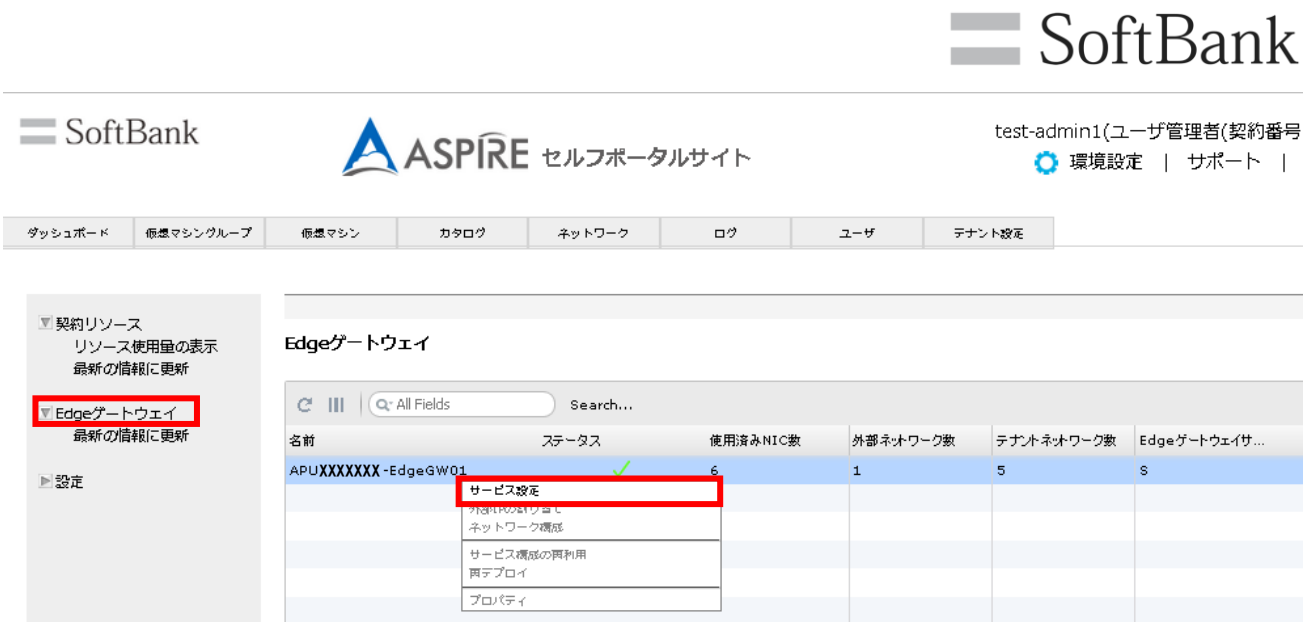
3.3.1. VPN 設定

(1). Web ブラウザからホワイトクラウド ASPIRE のセルフサービスポータルへアクセスし、ユーザ名とパスワードを入力してログインします。

(2). 2 段階認証に設定したパターンの場所の数字を入力し、ログインをクリックします。

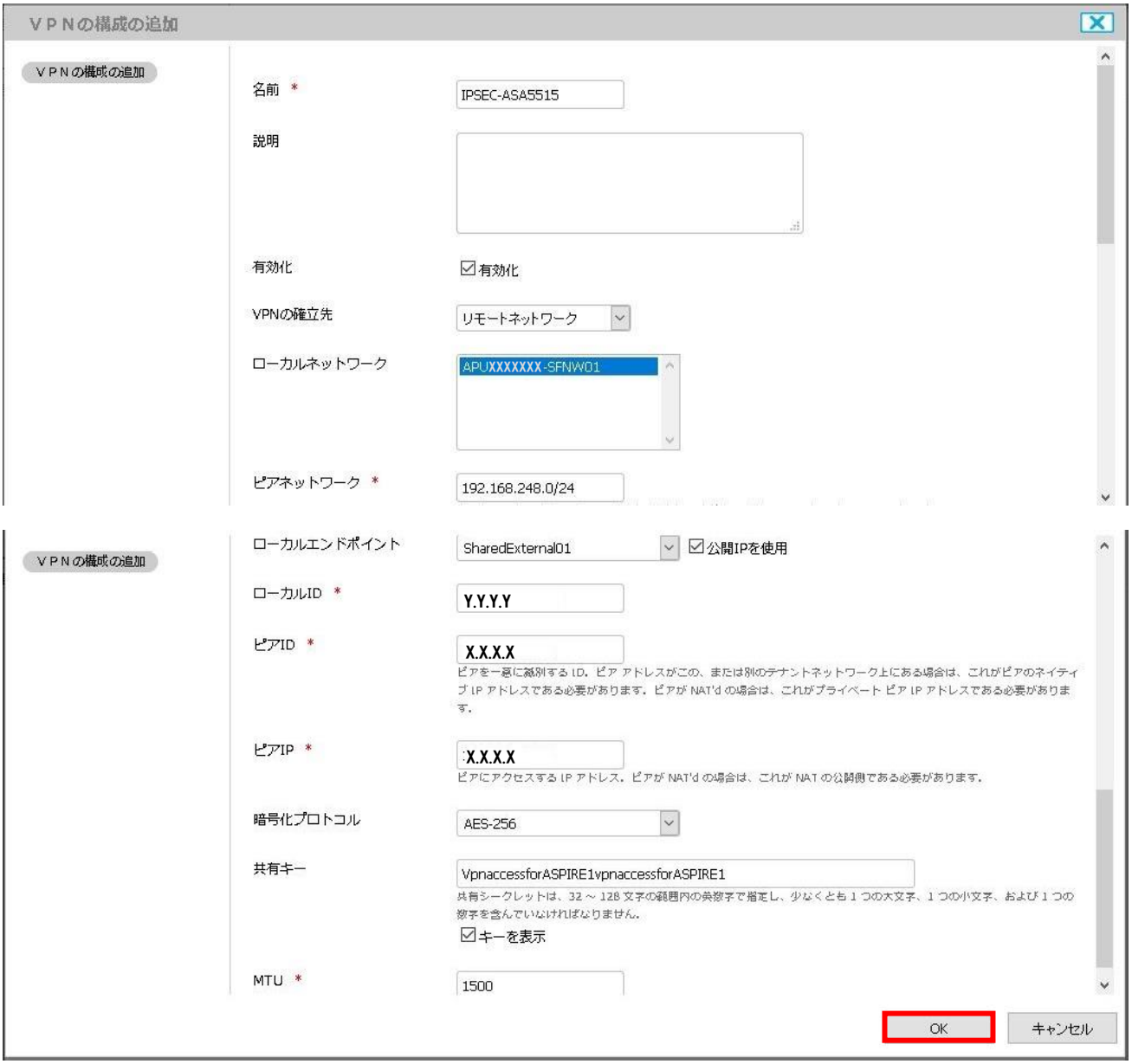
(3). テナント設定をクリックします。

(4). 左側のメニューより「Edge ゲートウェイ」 をクリックします。表示された Edge ゲートウェイ名（本資料では APUXXXXXXX-EdgeGW01）を右クリックし、「サービス設定」 をクリックします。



(5). 左側のメニューより「VPN」をクリックします。「VPN を有効化」のチェックボックスを有効化し、「追加」をクリックします。

(6). VPN パラメータを入力し、「OK」をクリックします。



名前 ： 任意 （本設定では IPSEC-ASA5515）

説明 ： 任意

有効化 ： チェックボックス をオン

VPN の確立先 ： リモート ネットワーク を選択

ローカルネットワーク ： ホワイトクラウド ASPIRE の VPN 接続対象 NW を選択

（本設定では APUXXXXXXX-SFNW01）

ピアネットワーク ： オンプレミスの VPN 接続対象 NW を指定（本設定では 192.168.248.0/24）

ローカルエンドポイント ：Edge ゲートウェイが接続している共有インターネット接続ネットワーク名を選択

（本設定では SharedExternal01）

ローカル ID： ホワイトクラウド ASPIRE のグローバル IP アドレス

ピア ID： オンプレミスの ASA5515 のグローバル IP アドレス（本設定では X.X.X.X）

ピア IP：オンプレミスの ASA5515 のグローバル IP アドレス（本設定では X.X.X.X）
暗号化プロトコル ：AES-256
共有キー ：3.2.2. の(5).で設定した事前共有キーを指定
（本設定では vpnaccessforASPIRE1vpnaccessforASPIRE1）
キーの表示 ： 無効を推奨（共有キーの内容確認のため一時的に ON にする場合以外は OFF を推奨）
MTU：1500

（7）. VPN 設定が完了しました。しかし、この時点ではまだ VPN 設定は Edge ゲートウェイに反映されていません。引き続きファイアウォールを設定します。

3.3.2. ファイアウォール設定

（1）. オンプレミスとホワイトクラウド ASPIRE の VPN 対象 NW 間の通信を許可するファイアウォール設定を追加します。「ファイアウォール」 より 「追加」 をクリックします。

（2）.ポップアップしたウィザード内へオンプレミスからホワイトクラウド ASPIRE への通信（Inbound）を許可するパラメータを入力し、「OK」ボタンをクリックします。

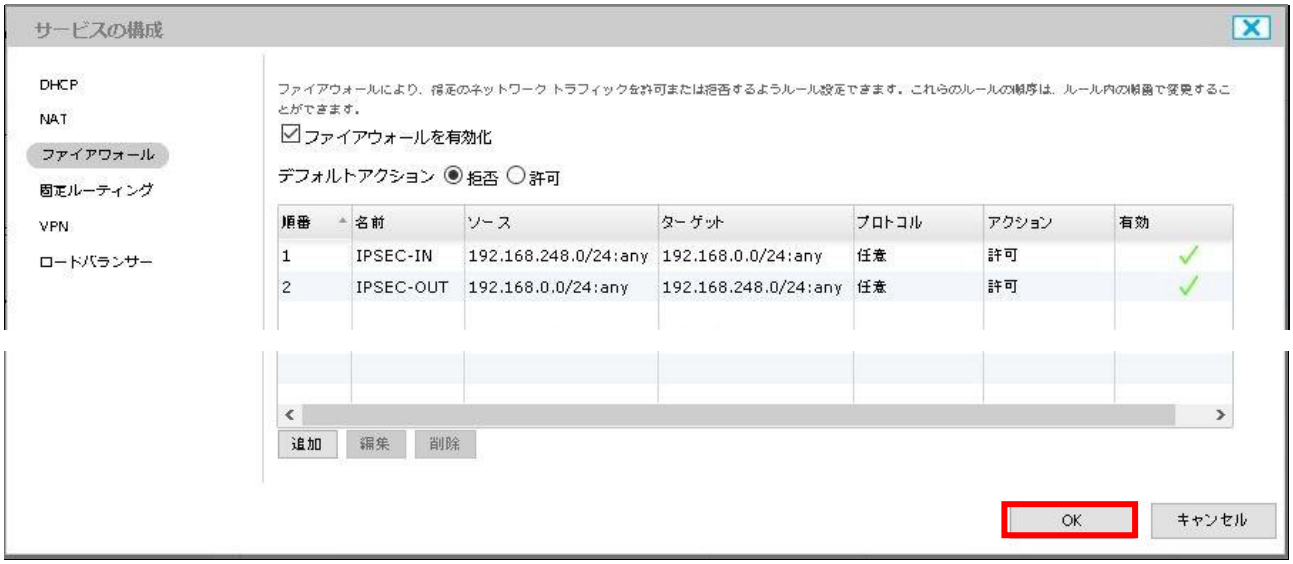
有効 ： チェックボックスをオン
名前 ： 任意（本設定では IPSEC-IN）
順番 ： 任意 （重複しない番号を割り当て）
ソース ： オンプレミスの VPN 接続対象 NW を指定 （本設定では、192.168.248.0/24）
ソースポート ： 任意 （本設定では、ANY）
ターゲット ： ホワイトクラウド ASPIRE の VPN 接続対象 NW を指定 （本設定では、192.168.0.0/24）
ターゲットポート ： 任意 （本設定では、ANY）
プロトコル ： 任意
アクション ： 許可

（3）. 続いて、反対方向の通信のファイアウォール設定を追加します。「追加」 をクリックします。

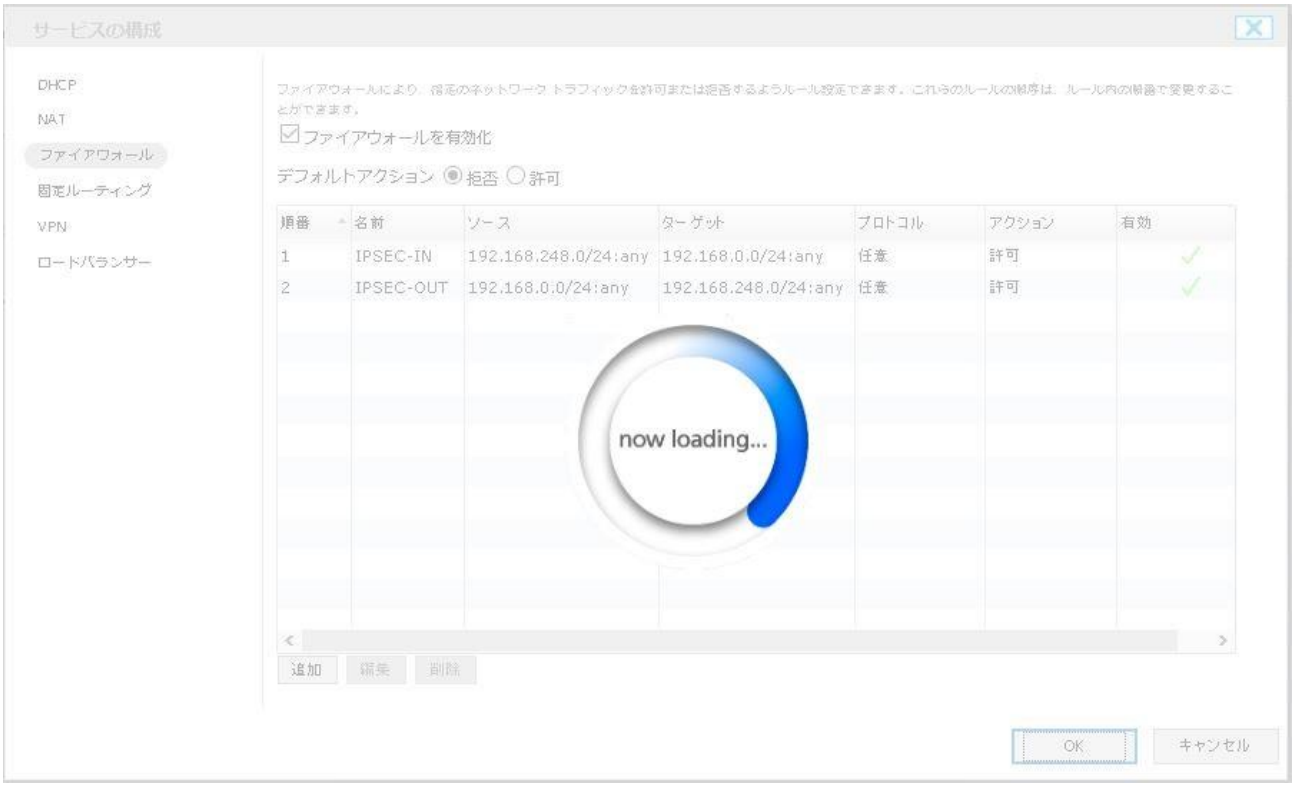
（4）. ポップアップしたウィザード内にホワイトクラウド ASPIRE からオンプレミスへの通信（Outbound）を許可するパラメータを入力し、「OK」ボタンをクリックします。

有効 ： チェックボックスをオン
名前 ： 任意（本設定では IPSEC-OUT）
順番 ： 任意（重複しない番号を割り当て）
ソース ： ホワイトクラウド ASPIRE の VPN 接続対象 NW を指定（本設定では、192.168.0.0/24）
ソースポート ： 任意（本設定では、ANY）
ターゲット ： オンプレミス側 VPN 接続対象 NW を指定（本設定では、192.168.248.0/24）
ターゲットポート ： 任意（本設定では、ANY）
プロトコル ： 任意
アクション ： 許可

（5）. VPN 設定とファイアウォール設定をホワイトクラウド ASPIRE へ反映させる為、「OK」をクリックします。



（6）.完了するまで待機します。変更は数秒で完了します。



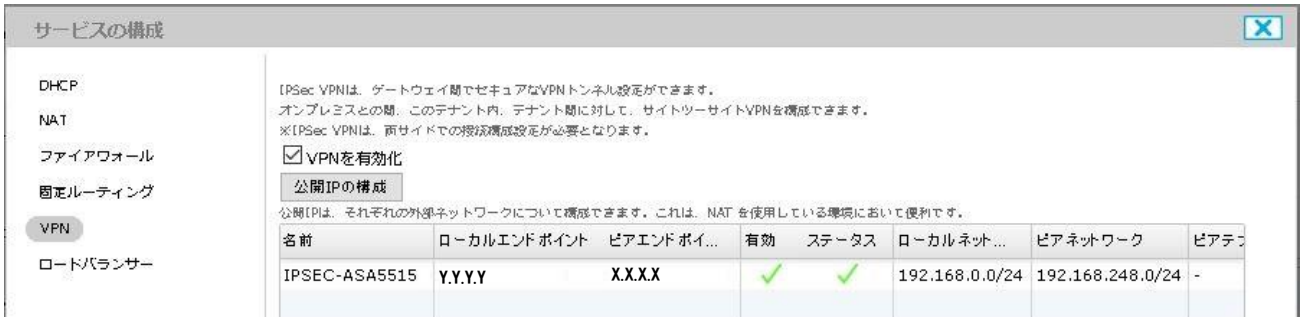
（7）.設定が完了しました。

3.4. VPN 接続後の通信確認

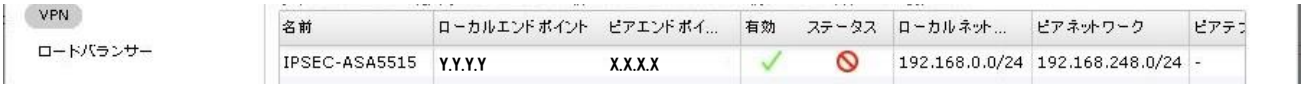
オンプレミスとホワイトクラウド ASPIRE の VPN 接続対象 NW の間で通信が行えることを確認します。

3.4.1. ホワイトクラウド ASPIRE セルフサービスポータルから確認

ホワイトクラウド ASPIRE のセルフサービスポータルより「Edge ゲートウェイ」へアクセスします。「サービス設定」より「VPN」を表示し、以下のように「ステータス」に緑色のチェックが表示されていれば、VPN 接続は正常に確立されています。



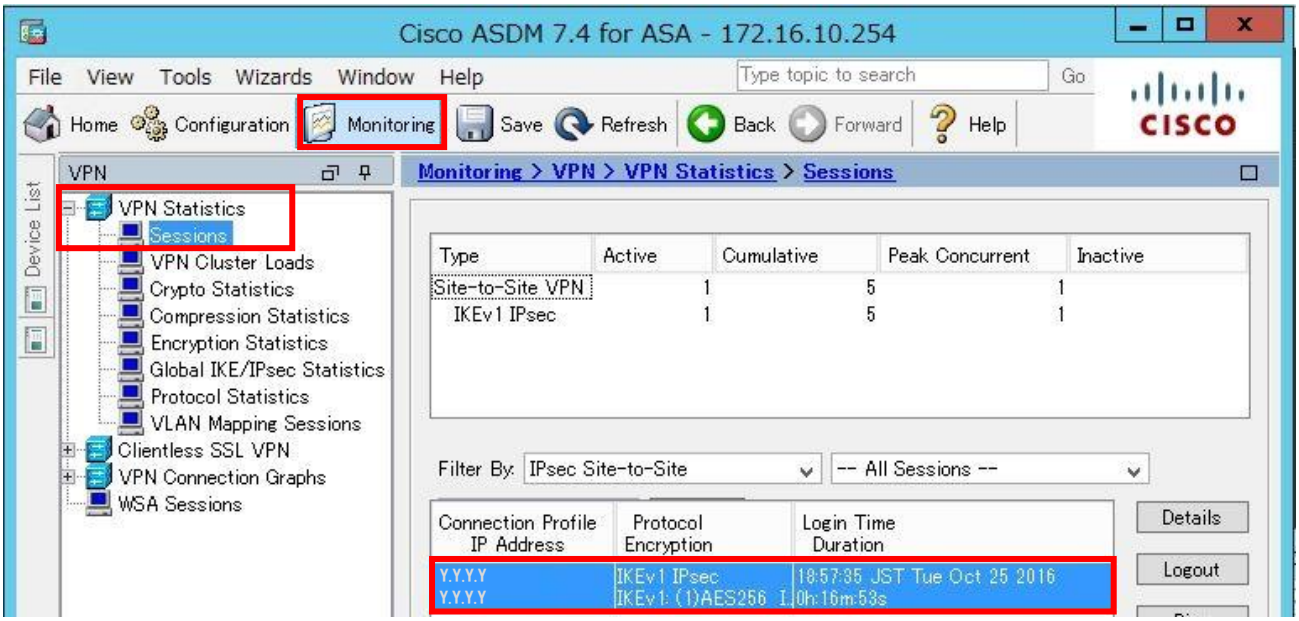
以下のように、「ステータス」表示に異常を示す赤色のマークが表示されている場合は、ASA5515、もしくはホワイトクラウド ASPIRE の VPN 設定に誤りがないかを確認して下さい。（※1）
VPN 確立先のアドレスや VPN 接続対象 NW、暗号化設定（事前共有キーやアルゴリズムの選択）に誤りがある場合、VPN 接続が正常に確立できません。



※1 ： VPN 接続が正常に確立されるまで多少時間が必要な場合があります。

3.4.2. Cisco ASDM から確認

「Monitoring」より「VPN Statistics」を展開し、「Sessions」をクリックします。
以下のように表示されていれば、VPN 接続は正常に確立されています。

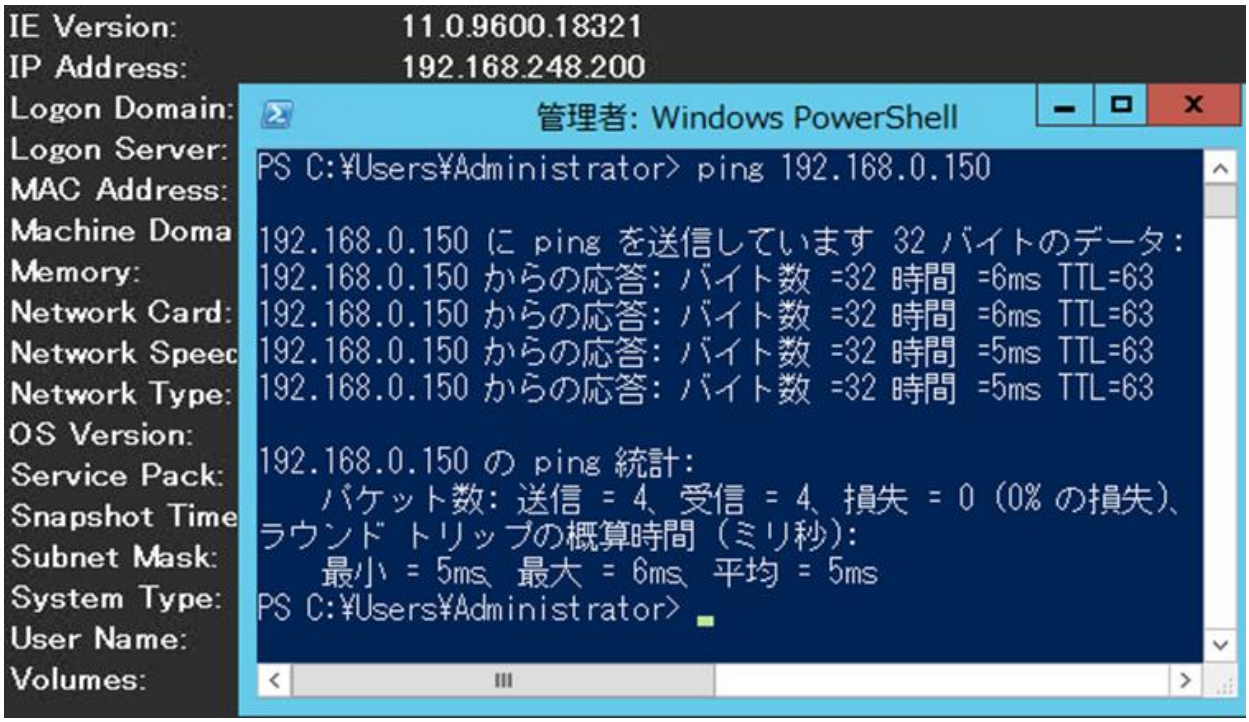


3.4.3. 仮想マシンから確認

オンプレミス、ホワイトクラウド ASPIRE 双方の VPN 接続対象 NW 上の仮想マシンから ping やリモートアクセスなどを実行し、双方間での疎通確認を行います。

（オンプレミス側からの確認例）

下記はオンプレミスの VPN 接続対象 NW 上の仮想マシン（Windows）から ping を実行した確認例です。

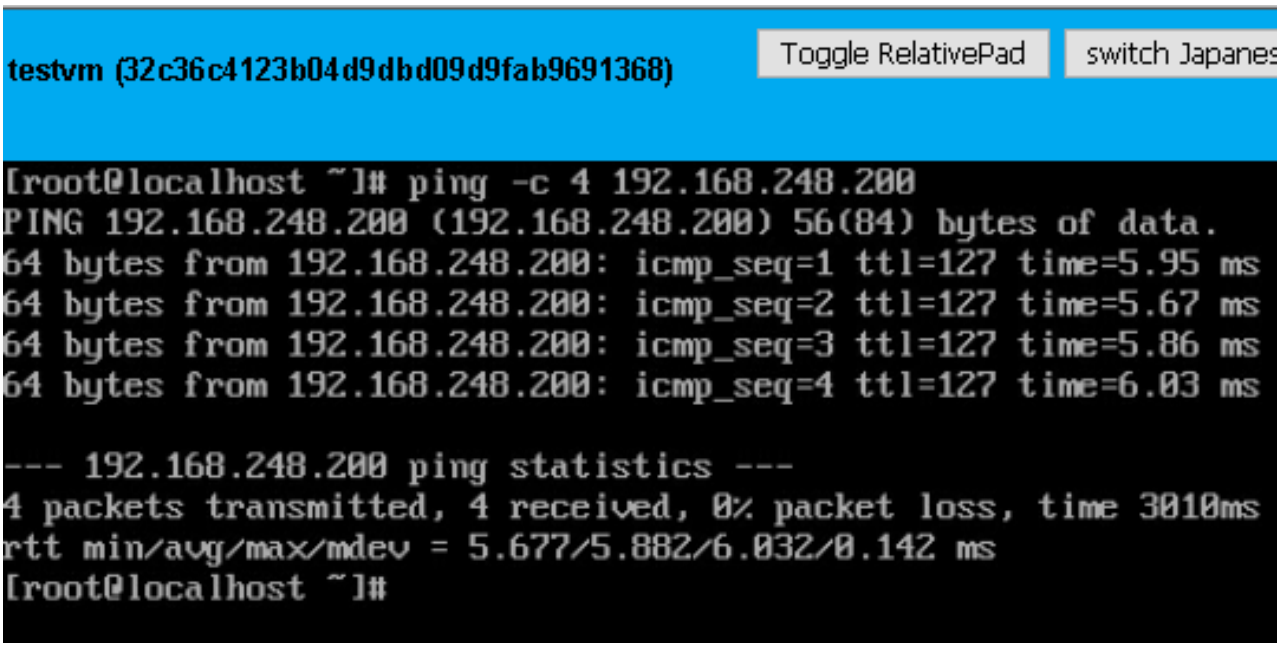


（ホワイトクラウド ASPIRE 側からの確認例）

ホワイトクラウド ASPIRE のセルフポータルサイトから「仮想マシン」をタブをクリックし、対象の仮想マシンを右クリックして「コンソールを開く」をクリックします。

ポップアウトしたコンソール内をクリックし、必要に応じてログイン操作等を行います。コンソールよりオンプレミスの仮想マシンへ通信ができることを確認します。

下記は Linux から ping を実行した確認例です。



ホワイトクラウド ASPIRE への IPsec VPN 接続手順は以上です。

3.5. 参考資料

3.5.1. 参考:本設定での ASA5515Config設定(抜粋)

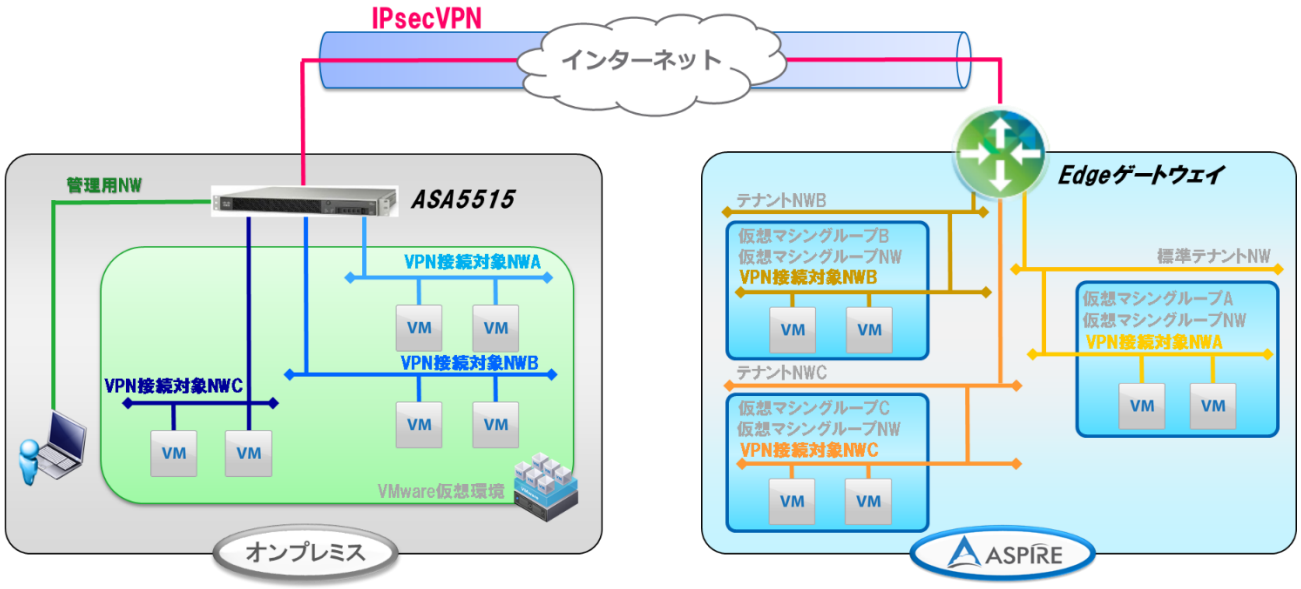
```
: Hardware:   ASA5515, 8192 MB RAM, CPU Clarkdale 3058 MHz, 1 CPU (4 cores)
ASA Version 9.2(3)4
!
interface GigabitEthernet0/0
 nameif to-Internet
 security-level 0
 ip address X.X.X.X 255.255.255.248
!
interface GigabitEthernet0/1
 nameif Local
 security-level 99
 ip address 192.168.248.253 255.255.255.0
!
interface Management0/0
 management-only
 nameif Management
 security-level 100
 ip address 172.16.10.254 255.255.255.0
!
object network Local_192.168.248.0_24
 subnet 192.168.248.0 255.255.255.0
object network CloudNW_192.168.0.0_24
 subnet 192.168.0.0 255.255.255.0
 description WhiteCloudASPIRE-NW
access-list Local_access_in_1 extended permit ip object Local_192.168.248.0_24 any
access-list to-Internet_cryptomap_1 extended permit ip object Local_192.168.248.0_24 object
CloudNW_192.168.0.0_24
!
nat (Local,to-Internet) source static Local_192.168.248.0_24 Local_192.168.248.0_24 destination static
CloudNW_192.168.0.0_24 CloudNW_192.168.0.0_24 no-proxy-arp route-lookup
!
object network Local_192.168.248.0_24
 nat (any,to-Internet) dynamic interface
```

```
!
route to-Internet 0.0.0.0 0.0.0.0 X.X.X.1 1
!
## 本設定に利用しない暗号化方式は記載していません
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec security-association lifetime seconds 3600
crypto ipsec security-association lifetime kilobytes unlimited
crypto ipsec security-association pmtu-aging infinite
crypto map to-Internet_map 1 match address to-Internet_cryptomap_1
crypto map to-Internet_map 1 set pfs
crypto map to-Internet_map 1 set peer Y.Y.Y.Y
crypto map to-Internet_map 1 set ikev1 transform-set ESP-AES-256-SHA
crypto map to-Internet_map 1 set security-association lifetime seconds 28800
crypto map to-Internet_map 1 set security-association lifetime kilobytes unlimited
crypto map to-Internet_map interface to-Internet
crypto ca trustpool policy
crypto ikev1 enable to-Internet
crypto ikev1 policy 30
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
group-policy GroupPolicy_Y.Y.Y.Y internal
group-policy GroupPolicy_Y.Y.Y.Y attributes
 vpn-tunnel-protocol ikev1
tunnel-group Y.Y.Y.Y type ipsec-l2l
tunnel-group Y.Y.Y.Y general-attributes
 default-group-policy GroupPolicy_Y.Y.Y.Y
tunnel-group Y.Y.Y.Y ipsec-attributes
 ikev1 pre-shared-key <Pre-Shared Key>
 isakmp keepalive disable
 ikev2 remote-authentication pre-shared-key <Pre-Shared Key>
 ikev2 local-authentication pre-shared-key <Pre-Shared Key>
!
```

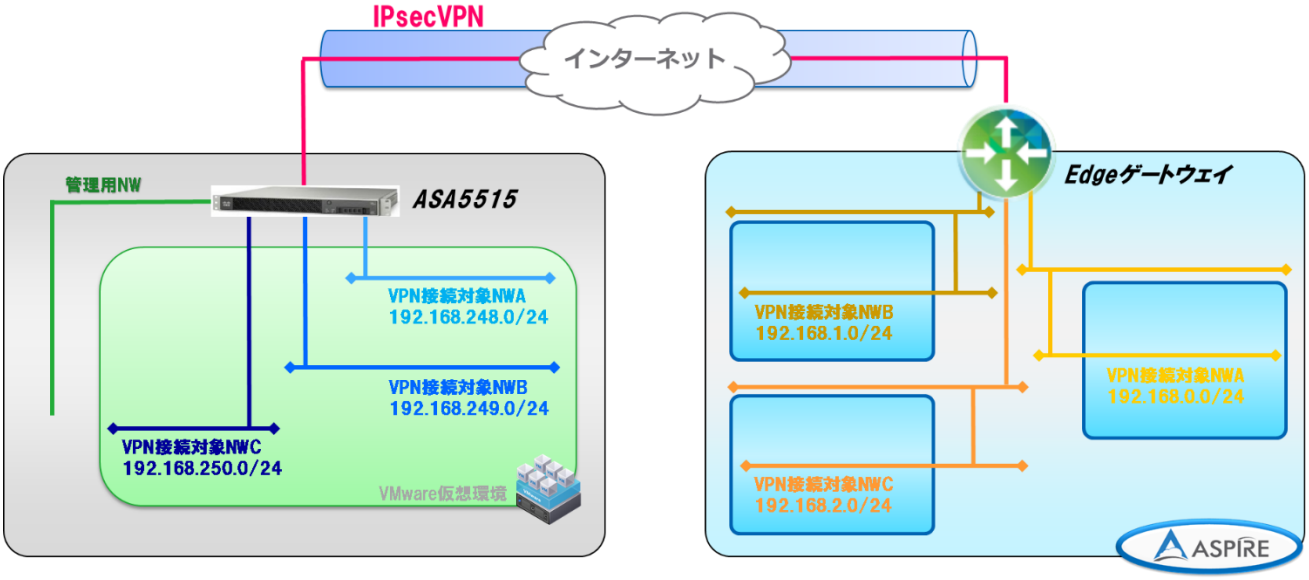
3.5.2. 参考:ASA5515 を用いて複数セグメント間で IPsec VPN を設定する場合

下記のように複数のネットワーク間で IPsec VPN を設定することもできます。
参考としてホワイトクラウド ASPIRE 側の3つのネットワークとオンプレミス側の3つのネットワーク間で IPsec VPN を構築する例を記載します。

・論理構成図



・ネットワーク図

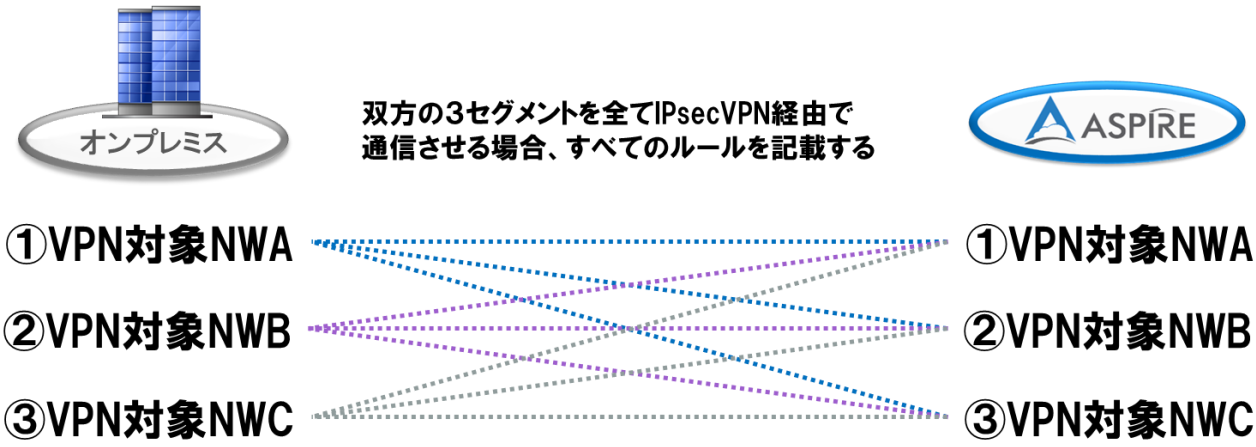


・設定概念図

ASA5515　　Edgeゲートウェイ

ホワイトクラウドASPIREのEdgeゲートウェイのIPsecVPN方式は、ポリシーベースVPNです。
IPsecVPN通信を構成したいトラフィックのルールを全て設定します。

構成例



3.5.2.1. 複数セグメント間での IPsec VPN 設定（ASA5515）

Cisco ASDM より複数セグメント間での IPsec VPN を設定する場合の異なる設定箇所を記載します。

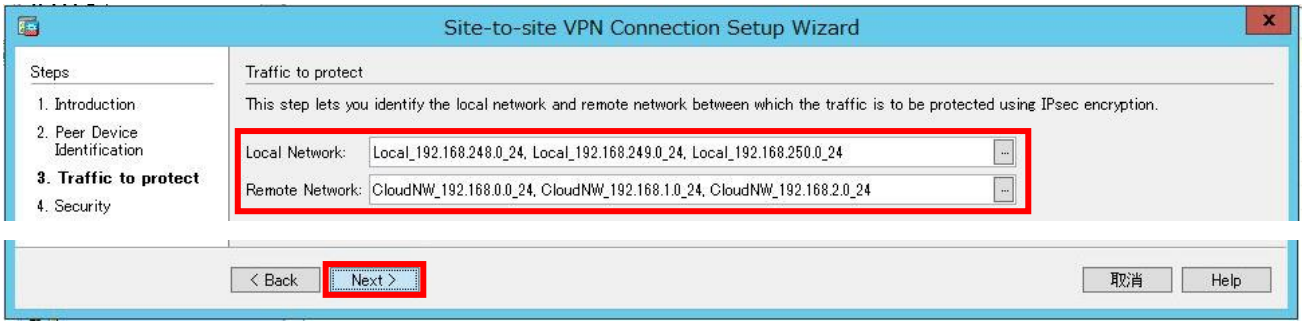
・ファイアウォール　オブジェクト設定

VPN 接続対象 NW を全て登録します。

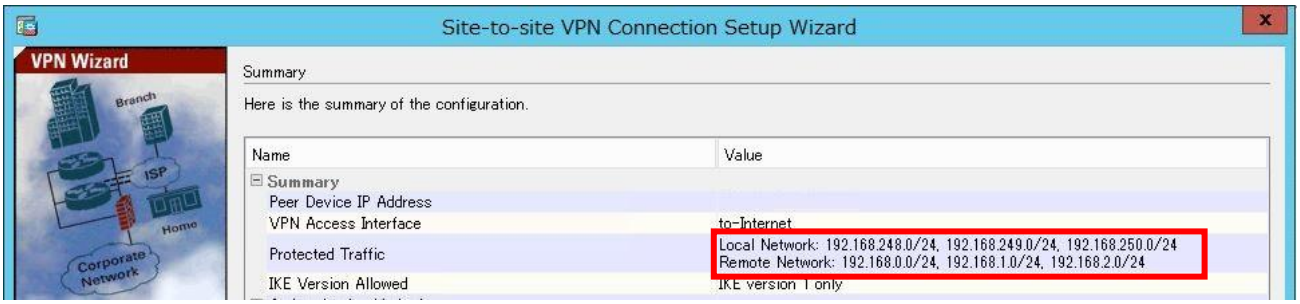
CloudNW_192.168.0.0_24	192.168.0.0	255.255.255.0	WhiteCloudASPIRE-NW	
CloudNW_192.168.1.0_24	192.168.1.0	255.255.255.0		
CloudNW_192.168.2.0_24	192.168.2.0	255.255.255.0		
Local_192.168.248.0_24	192.168.248.0	255.255.255.0		to-Internet (P)
Local_192.168.249.0_24	192.168.249.0	255.255.255.0		to-Internet (P)
Local_192.168.250.0_24	192.168.250.0	255.255.255.0		to-Internet (P)

・VPN 設定

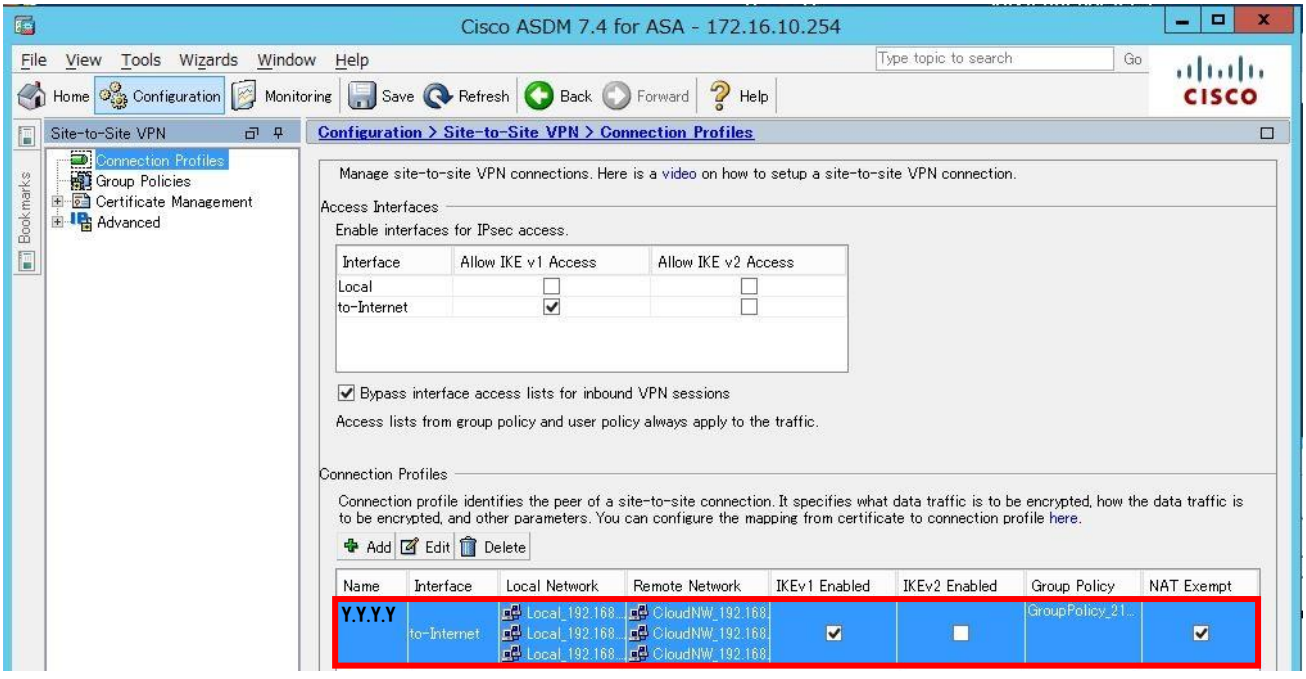
(1). VPN ウィザードの 3STEP 目の「Traffic to protect」で VPN 接続対象 NW を全て設定し、「Next」 をクリックします。



(2). 設定確認画面にて VPN 接続対象 NW が全て含まれていることを確認します。



(3). VPN 設定の微調整を実施していない場合は同様に実施します。



3.5.2.2. 複数セグメント間での IPsec VPN 設定 （ホワイトクラウド ASPIRE）

ホワイトクラウド ASPIRE のセルフポータルサイトより複数セグメント間での IPsec VPN を設定する場合の異なる設定箇所を記載します。

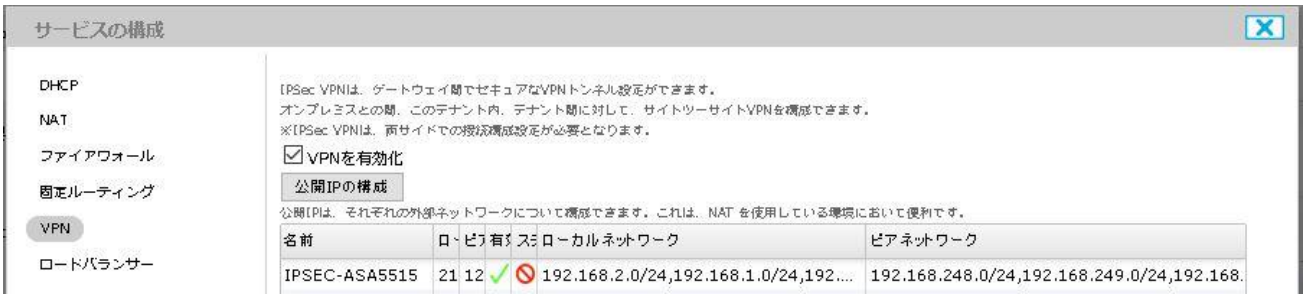
・VPN 設定

(1). VPN の構成の追加時に設定する VPN を全て選択します。

ローカルネットワーク ： Ctrl キーを押しながら、設定したいテナントネットワーク名を選択

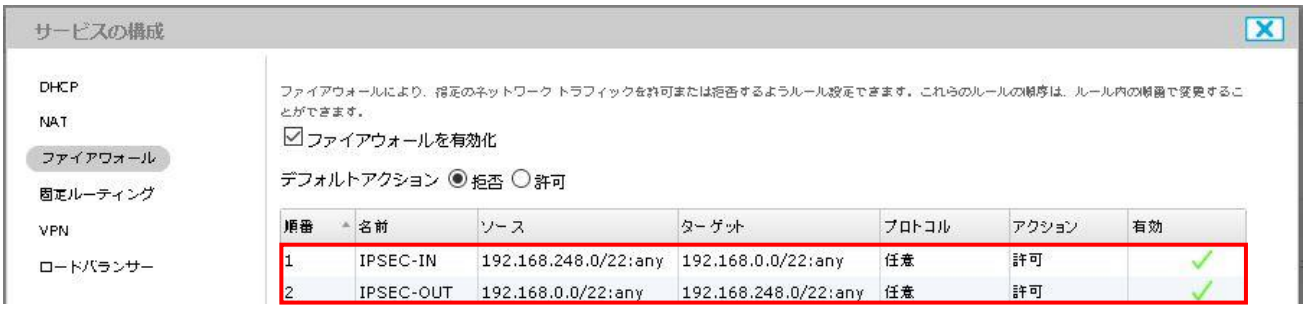
ピアネットワーク ： 設定するネットワークを “ , ”（カンマ）で区切ります。

(2). 設定した対象 NW を下記のように確認できます。



・ファイアウォール設定

（1）. 通信させたいすべてのトラフィックルールをファイアウォールに設定します。

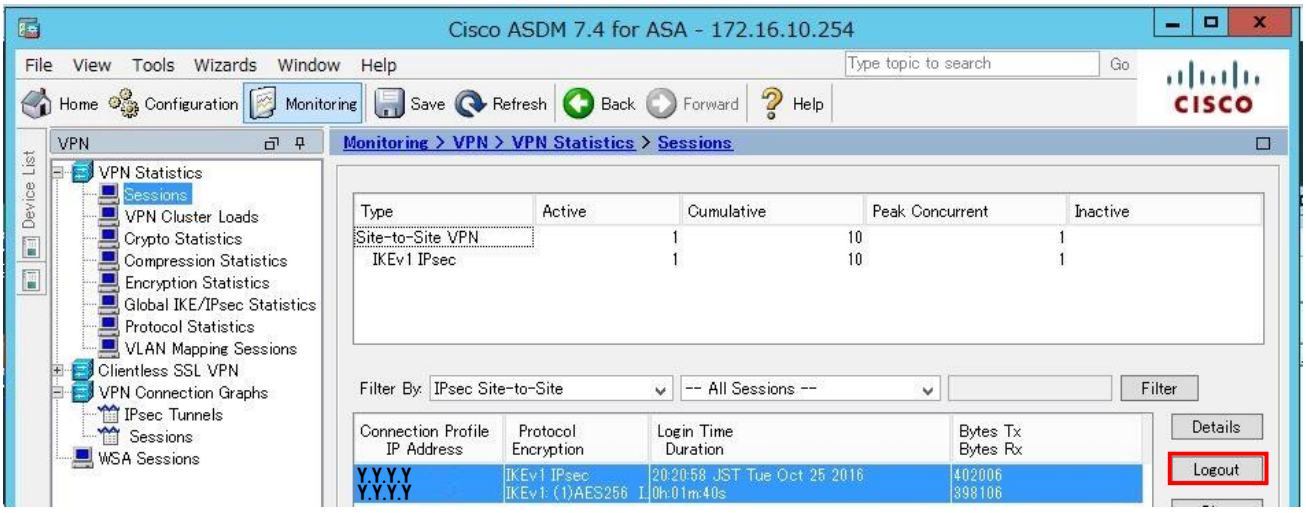


本資料の構成ですべてのトラフィックルールを VPN 対象 NW 毎に設定すると、
最低でも ３ × ３ × ２（In/Out） = 18 本のルール設定が必要です。
ネットワークをサマライズすることで設定本数を減らすことができます。

3.5.2.3.VPN 接続後の通信確認時の注意点

稀に ASPIRE 上のステータスが有効となっていても双方での IPsec VPN のネゴシエーションの一部が失敗し、その一部のルールの通信が不可となるケースがあります。
その場合は、オンプレミスのネットワーク機器で IPsec VPN の SA を削除してください。

ASA5515 の場合は Cisco ASDM より「Monitoring」、「VPN Statistics」、「Sessions」より「Logout」をクリックすることで SA を削除できます。



以上