

mGuard シリーズ Q & A

Innominate 社日本総代理店
アルテック・エーディエス株式会社
オプト&ネットワーク事業部
www.e-security-ads.com
e-security-ads@altech.co.jp

目次:

- 1. Configuration.....5
 - 1.1 General Questions.....5
 - No 1.1.1 mGuard は Route コマンドと netstat コマンドをサポートしていますか？5
 - No 1.1.2 mGuard を使用する時にドライバーのインストールが必要ですか？5
 - No 1.1.3 mGuard のマニュアル及び参考コンフィグはありませんか？5
 - No 1.1.4 ネットワーク・モード(ステルス / ルーター / PPPoE | PPTP)について、教えてください。5
 - No 1.1.5 mGuard スマートにおいて、中央の LED が赤く点滅をしています、どうしたらよいでしょうか？6
 - No 1.1.6 MTU サイズを変えるのは可能ですか？6
 - No 1.1.7 クロスケーブルを使用する必要がありますか？6
 - No 1.1.8 ISDN を直接 mGuard に接続できますか？7
 - No 1.1.9 WINS サーバを指定するのは可能ですか？7
 - No 1.1.10 NAT(Network Address Translation)とは、何ですか？7
 - No 1.1.11 NAT-T(Network Address Translation Traversal)とは何ですか？7
 - No 1.1.12 HTTPS 設定をして、リモートアクセスを可能にしましたが、アクセスができません。7
 - 1.2 Stealth mode.....8
 - No 1.2.1 Stealth モードとは何ですか？8
 - No 1.2.2 Stealth モードの自動設定 / 手動設定 / マルチクライアント の違いを教えてください。8
 - No 1.2.3 mGuard が保護しているクライアントに対して Ping 通信ができません。8
 - No 1.2.4 https://1.1.1.1 にて mGuard にアクセスすることができません。9
 - No 1.2.5 クライアント PC から mGuard へログインする為に、クライアント PC は mGuard(IP=1.1.1.1)と同じ9
ネットワークに設定する必要がありますか？9
 - No 1.2.6 なぜデフォルトゲートウェイを指定する必要がありますか？9
 - No 1.2.7 WEB ブラウザエラーメッセージ、「Unknown host 1.1.1.1」9
 - No 1.2.8 mGuard に対してリモートアクセスができますか？ その時にどの IP アドレスを使用すれば良いの10
でしょうか？10
 - 1.3 Router mode (PPPoE / PPTP).....10
 - No 1.3.1 mGuards の外部 IP アドレスが「ping」が可能ではありません。10
 - No 1.3.2 内部ルータの追加及び外部ルータの追加は、どういう時に使用するのでしょうか？10
 - No 1.3.3 WEB ブラウザから mGuard にアクセスすることができません。10
 - No 1.3.4 PPPoE モードで、インターネットへアクセスができません。10
- 2 Software Update, Recovery- and Flash Procedure.....11
 - 2.1 Software Update11
 - No 2.1.1 ソフトウェアアップデートを実行するとき、mGuard で設定された構成プロファイルが消えてしまいますか？11

- No 2.1.2 オフライン・アップデートで以下のメッセージが表示されました。 11
 - “ tar: Invalid gzip magic ” 11
- No 2.1.3 オンライン・アップデートで以下のメッセージが表示されました。 11
 - “ Not a valid hostname or IP address “ 11
- No 2.1.4 オンライン・アップデートで以下のメッセージが表示されました。 11
 - “ 404: HTTP/1.0 404 Not Found “ 11
- No 2.1.5 オンライン・アップデートで以下のメッセージが表示されました。 12
 - “ HTTP/1.0 401 Authorization Required “ 12
- No 2.1.6 アップデート中に以下のメッセージが表示されました。 12
 - “ Update message 35 packages not installed completely “ 12
- No 2.1.7 アップデート中に以下のメッセージが表示されました。 12
 - “ Update message 1 package not installed completely Please reboot “ 12
- 2.2 Recovery Procedure 13
 - No 2.2.1 リカバリは、どういう状況の時に使用するのでしょうか？ 13
 - No 2.2.2 リカバリを実行すると、設定された構成プロファイルは消去されてしまいますか？ 13
- 2.3 Flash Procedure 13
 - No 2.3.1 フラッシングは、どういう状況で行なうのでしょうか？ 13
 - No 2.3.2 フラッシングの手順を教えてください。 13
 - No 2.3.3 Windows TFTP/DHCP サーバに関する問題 13
 - No 2.3.4 DHCP サーバが IP アドレスを送った後に中央 LED は赤く点灯します。 14
 - No 2.3.5 以下のエラーメッセージが表示されます。 14
 - “ The system cannot find the file specified (rollout.sh) “ 14
- 3 VPN 15
 - 3.1 General Questions 15
 - No 3.1.1 10 VPN トンネル とは？ VPN トンネル数ですか又 IP のコネクション数ですか？ 15
 - No 3.1.2 事前共有鍵シークレット (PSK) を使用できる状況は？ 15
 - No 3.1.3 Dead Peer Detection (DPD) とは？ 15
 - No 3.1.4 両方の mGuardn の間に NAT ゲートウェイが設置されている場合、どういう設定が必要でしょうか？ 15
 - 3.2 VPN Tunnel Problems 16
 - No 3.2.1 DynDNS を使用して VPN トンネルを設定する時に、確立することができません。 16
 - No 3.2.2 DynDNS を使用する VPN トンネルが 2、3 時間後に中断されます。 16
 - No 3.2.3 VPN トンネルが確立できましたが、片方向しか通信ができません。 16
 - No 3.2.4 VPN トンネルを確立することができません。 理由は何でしょうか？ 16
 - No 3.2.5 VPN 接続を確立することができません。また、ipsec daemon は始動されません。 16
 - No 3.2.6 以下のメッセージが表示されました。 17
- 4 Firewall 18
 - No 4.1 ファイヤーウォールの設定をする時に必要なことを教えてください。 18

No 4.2 インカミング・ルール設定は必要でしょうか？ 18

No 4.3 インターネットへのアクセスを防ぎたいと思いますが、正常に動作をしません。 18

No 4.4 クライアント PC から mGuard までの ICMP Echo Request は、ファイヤーウォールのログに表示されません。 18

No 4.5 ファイヤーウォールのインカミング設定で全て「拒否」の設定の時にポートフォワーディングで、 18
クライアント PC に対して通信ができてしまう。 18

No 4.6 MAC フィルタの設定にて一定の PC からのみ通信を許可にしたが、設定していない PC からも 19
通信ができてしまう。 19

No 4.7 1:1NAT は、どういう状況で使用するのでしょうか？ 19

No 4.8 ファイヤーウォールのスループットが不十分 21

5 Services 21

No 5.1 NTP サーバを設定して、NTP サービスを可能にしましたが、正常に動作をしません。 21

No 5.2 DHCP リレーに関する問題 21

6 Anti Virus Protection (AVP) 22

No 6.1 アンチウイルスのライセンスについて教えてください。 22

No 6.2 mGuard で「5Mbyte 以上ブロックする」の設定の時に添付ファイル:5Mbyte 以上を受信した場合 22
スキャンすることができないので、その後のメールが受信できなくなる。 22

No 6.3 AVP データベースをアップデートするときの問題 22

7 Third Party Products 23

No 7.1 ステルス・モードで使用 : TFTP を使用したシスコの機器のファーム・アップができません。 23

No 7.2 mGuard は、IPX をサポートしていますか？ 23

変更履歴

バージョン	日付	コメント
Ver 1.0	2006/03/31	新規作成

1. Configuration

1.1 General Questions

No 1.1.1 mGuard は Route コマンドと netstat コマンドをサポートしていますか？

回答： Route コマンド 及び netstat コマンドをサポートしていません。

しかし、mGuard は iproute2 情報を表示できます。

No 1.1.2 mGuard を使用する時にドライバーのインストールが必要ですか？

回答： mGuard PCI をドライバー・モードで使用する時のみ、ドライバーのインストールが必要です。

ドライバー提供のサポート: Windows XP/2000 , Linux

No 1.1.3 mGuard のマニュアル及び参考コンフィグはありませんか？

回答： アルテック・エーディエス e-セキュリティ事業部のホームページからダウンロードができます。

(<http://www.e-security-ads.com>)

mGuard マニュアル、 mGuard 設定例 等

No 1.1.4 ネットワーク・モード(ステルス / ルーター / PPPoE | PPTP)について、教えてください。

回答：

ステルス・モード

mGuard がステルス・モードで設定されている時は、クライアントの設定を再構成する必要はありません。保護が必要とされるクライアント PC と mGuard の内部インターフェースを接続します。

その時にクライアント PC の IP アドレスを変更する必要がありません。

また、mGuard は透明な状態で動作し、ポートスキャンでも検出をしません。

ステルス・モード : 自動設定、手動設定、マルチクライアント

保護する PC が一つの場合は、自動設定又は手動設定が選択されます

保護する PC が複数の場合は、マルチクライアントが選択されます。

mGuard ステルス・モード:自動設定を使用している場合は、内部のネットワークからのパケットを分析することにより、クライアント PC の IP アドレスを採用して、自動的に IP アドレスを検出します。

mGuard ステルス・モード:手動設定をしている場合は、内部のネットワークからのパケット送信がない状態の時にクライアント PC の IP アドレス / MAC アドレス を設定することにより mGuard はクライアント PC の IP アドレスを採用し、保護します。

mGuard ステルス・モード:マルチステルス・モードを設定している場合は、内部ネットワークに複数のクライアント PC が接続されている状態時に選択され、管理 IP アドレスを設定します。

ルーター・モード

mGuard ルーター・モードは、2つのネットワーク間のルータとして使用できます。

その際に内部ネットワーク及び外部ネットワークインターフェースの設定をする必要があります。

PPPoE/PPTP・モード

mGuard PPPoE / PPTP モードは、mGuard は内部のネットワークとインターネット間の DSL ルータとして機能します。

mGuard の外部のインタフェースは、DSL モデムに接続される必要があります、内部のインタフェースを構成する必要があります。

No 1.1.5 mGuard スマートにおいて、中央の LED が赤く点滅をしています、どうしたらよいでしょうか？

回答: 中央の LED が赤く点滅状態の場合は、カーネルによって使用されるいくつかのファイルが欠けているので、mGuard は起動しないかもしれません。ファーム・アップデート又はファームウェア・フラッシング中に電源を中断した場合に起こることがあります。再度、ファームウェア・フラッシングをすることによって、この問題を解決できます。

No 1.1.6 MTU サイズを変えるのは可能ですか？

回答: バージョン 3.0.0 から mGuard メニュー -> ネットワーク -> 拡張設定で MTU サイズを変えるのは可能になりました。

No 1.1.7 クロスケーブルを使用する必要がありますか？

回答: かならずしも、必要とはしません。mGuard は、自動的に接続ケーブルのタイプと転送レートを検出します。(AUTO MDI/MDX 対応)

No 1.1.8 ISDN を直接 mGuard に接続できますか？

回答：いいえ、できません。mGuard のコネクタはイーサネット接続だけをサポートしています。

No 1.1.9 WINS サーバを指定するのは可能ですか？

回答：mGuard メニュー -> サービス -> DHCP を使用して WINS サーバを指定するのは可能です。

No 1.1.10 NAT(Network Address Translation)とは、何ですか？

回答：インターネットに接続された企業などで、一つのグローバルな IP アドレスを複数のコンピュータで共有する技術。組織内でのみ通用する IP アドレス(ローカルアドレス)と、インターネット上のアドレス(グローバルアドレス)を透過的に相互変換することにより実現される。最近不足がちなグローバル IP アドレスを節約できるが、一部のアプリケーションソフトが正常に動作しなくなるなどの制約がある。

No 1.1.11 NAT-T(Network Address Translation Traversal)とは何ですか？

回答：VPNクライアントがNATの有無を確認した上で、ダミーのUDPヘッダをESPパケットに付け、ルーターのNAT/IP マスカレードで変換させるという機能です。

No 1.1.12 HTTPS 設定をして、リモートアクセスを可能にしましたが、アクセスができません。

回答：mGuard メニュー -> アクセス -> HTTPS のファイヤーウォール設定を確認してください、。

No 1.1.13 クライアントから mGuard を設定するためのリモート・アクセスを可能にする必要がありますか？

回答：いいえ。内部ネットワークからのアクセスの場合はデフォルトでアクセスができます。
内部ネットワークからのアクセスを禁止した場合は、必ず外部ネットワークからのアクセスを可能にしてください。内部 / 外部ネットワーク共にアクセスを禁止した場合は、リカバリを実施する必要があります。

1.2 Stealth mode

No 1.2.1 Stealth モードとは何ですか？

回答： mGuard 本体に IP アドレスを持ちません。

保護が必要とされるクライアント PC と mGuard の内部インターフェースを接続します。

mGuard は、内部ネットワークからの IP アドレスを認識して、使用します。

mGuard がステルス・モードで設定されている時は、クライアントの設定を再構成する必要はありません。

つまり、クライアント PC の IP アドレスを変更する必要がありません。

また、mGuard は透明な状態で動作し、ポートスキャンでも検出をしません。

PPPoE 接続の場合は、ステルス・モードの使用はできません。

No 1.2.2 Stealth モードの自動設定 / 手動設定 / マルチクライアント の違いを教えてください。

回答： mGuard ステルス・モード:自動設定を使用している場合は、内部のネットワークからのパケットを分析することにより、クライアント PC の IP アドレスを採用して、自動的に IP アドレスを検出します。

mGuard ステルス・モード:手動設定をしている場合は、内部のネットワークからのパケット

送信がない状態の時にクライアント PC の IP アドレス / MAC アドレス を設定することにより mGuard はクライアント PC の IP アドレスを採用し、保護します。

mGuard ステルス・モード:マルチステルス・モードを設定している場合は、内部ネットワークに複数のクライアント PC が接続されている状態時に選択され、管理 IP アドレスを設定します。

No 1.2.3 mGuard が保護をしているクライアントに対して Ping 通信ができません。

回答： mGuard ファイヤーウォールのインカミング設定で ICMP が許可になっていることを確認してください。

クライアント PC 上でファイヤーウォールが有効になっていないかを確認してください。

(例:WindowsXP ファイヤーウォール)

クライアント PC 上で VPN クライアントソフトがインストールされていないかを確認してください。

(VPN クライアントソフトの中にはファイヤーウォール機能がついたソフトもあります)

No 1.2.4 <https://1.1.1.1> にて mGuard にアクセスすることができません。

回答：この場合の原因として、複数考えられますので、以下の項目を確認してください。

WEB ブラウザで、プロキシ設定がされている場合。

クライアント PC のファイヤーウォール機能によって、アクセスが拒否されている場合。

クライアント PC 上でデフォルトゲートウェイが設定されていない。

外部インターフェースがネットワークに接続されていない場合は、以下を確認してください。

mGuard の外部インターフェースがネットワークに接続されていない場合でも、クライアント PC の設定でデフォルトゲートウェイが設定されていること

ステルス・モード設定で、デフォルト・ゲートウェイが存在していない場合はクライアント PC 上で、ゲートウェイアドレスに対して、ARP 解決を行なってください。

(詳細は、アルテック・エーディエス e-セキュリティ事業部のホームページの mGuard 設定例 スタートアップを参照してください) <http://www.e-security-ads.com>

No 1.2.5 クライアント PC から mGuard へログインする為に、クライアント PC は mGuard(IP=1.1.1.1)と同じネットワークに設定する必要がありますか？

回答：いいえ。必要ありません。

mGuard へのログインで使用される IP=1.1.1.1 は擬似的な IP アドレスとなります。

No 1.2.6 なぜデフォルトゲートウェイを指定する必要がありますか？

回答：クライアント PC からゲートウェイ宛てに ARP 解決を行ないます。

ARP 解決後に、mGuard は、クライアント PC のアドレスを使用します。

つまり、ゲートウェイを指定しないと、mGuard はクライアント PC のアドレスを認識することができません。

外部インターフェースが接続されていない場合でもクライアント PC のゲートウェイは必要となります。

この場合は、クライアント PC 上で、ゲートウェイアドレスに対して ARP 解決を行ないます。

No 1.2.7 WEB ブラウザエラーメッセージ、「Unknown host 1.1.1.1」

回答：WEB ブラウザがプロキシを使用すると、このエラーメッセージが表示されます。

No 1.2.8 mGuard に対してリモートアクセスができますか？その時にどの IP アドレスを使用すれば良いのでしょうか？

回答： mGuard メニュー -> アクセス -> HTTPS（又は SSH）で設定をします。

この際に必ず、ファイヤーウォール設定を忘れずに設定してください。

リモートアクセスを行なう PC からは、mGuard が保護をしている IP アドレスを使用して、mGuard へログインします。

1.3 Router mode (PPPoE / PPTP)

No 1.3.1 mGuards の外部 IP アドレスが「ping」が可能ではありません。

回答： mGuard メニュー -> ファイヤーウォール -> 拡張設定 で「外部から mGuard への ICMP」の項目で ICMP を有効にしてください。

No 1.3.2 内部ルータの追加及び外部ルータの追加は、どういう時に使用するのでしょうか？

回答： 内部のネットワークが別のネットワークにアクセスする時に内部ルートを設定する必要があります。外部ルータの追加の場合も、内部と同様です。

No 1.3.3 WEB ブラウザから mGuard にアクセスすることができません。

回答： mGuard の内部 IP アドレスがクライアント PC のゲートウェイアドレスに設定されていることを確認します。 mGuard の内部アドレスが不明の場合は、mGuard リカバリが必要となります。

(詳細は、アルテック・エーディエス e-セキュリティ事業部のホームページの mGuard 設定例 リカバリを参照してください) <http://www.e-security-ads.com>

No 1.3.4 PPPoE モードで、インターネットへアクセスできません。

回答： NAT 機能が有効になっていることを確認してください。

クライアント PC の設定で、DNS サーバのアドレスが、プロバイダー指定のアドレスか、mGuard の内部 IP アドレスになっていることを確認してください。

2 Software Update, Recovery- and Flash Procedure

2.1 Software Update

No 2.1.1 ソフトウェアアップデートを実行するとき、mGuard で設定された構成プロファイルが消えてしまいますか？

回答： いいえ。ソフトウェアアップデートを実行しても、構成プロファイルは消去されません。
フラッシングを実行時には、mGuard は構成プロファイルを消去して、デフォルト設定になります。

No 2.1.2 オフライン・アップデートで以下のメッセージが表示されました。

“ tar: Invalid gzip magic ”

回答： アップデート・パッケージの拡張子が以下の形式であることを確認してください。
*.tar.gz (Internet Explorer の場合、 *.tar.tar として保存します)

No 2.1.3 オンライン・アップデートで以下のメッセージが表示されました。

“ Not a valid hostname or IP address “

回答： アップデートサーバ(update.innominate.com)の IP アドレスを取得できない状態の時に、このメッセージが表示されます。この場合、mGuard メニュー -> サービス -> DNS にて、DNS サーバを設定してください。
mGuard がステルス・モードで動作をしている場合は、クライアント PC のファイヤーウォールの設定を確認してください。外部からの ICMP リクエストを許可にすることによって、デフォルトゲートウェイの MAC アドレスを取得して、アップデートサーバとの通信ができるようになります。

No 2.1.4 オンライン・アップデートで以下のメッセージが表示されました。

“ 404: HTTP/1.0 404 Not Found “

回答： mGuard メニュー -> システム情報 -> アップデート・サーバのプロトコルの項目で、” https:// “ になっていることを確認してください。

No 2.1.5 オンライン・アップデートで以下のメッセージが表示されました。

“ HTTP/1.0 401 Authorization Required “

回答: mGuard メニュー -> システム情報 -> アップデート・サーバの項目で、ログインとパスワードを設定して下さい。

No 2.1.6 アップデート中に以下のメッセージが表示されました。

“ Update message 35 packages not installed completely “

回答: mGuard のアップデートで、最初に現在のパッケージとインストールしようとしているパッケージをチェックします。この情報に基づいていくつのパッケージをアップデートで必要かを決定して、必要のパッケージ数を表示します。

No 2.1.7 アップデート中に以下のメッセージが表示されました。

“ Update message 1 package not installed completely Please reboot “

回答: これは、エラーメッセージでは、ありません。

mGuard をリブートしてください。リブート終了後、アップデートは終了です。

2.2 Recovery Procedure

No 2.2.1 リカバリは、どういう状況の時に使用するのでしょうか？

回答：以下の状況の時に、mGuard のリカバリを実行する必要があります。

ルータモード又は PPPoE モードの時に、内部 IP アドレスが不明になった場合にリカバリは必要となります。
リカバリ実施後、以下の設定になります。

デルタの場合：デフォルトのルータモードになります。(ログイン:192.168.1.1)

スマート、ブレード、PCI の場合：ステルスモードになります。(ログイン:1.1.1.1)

管理 IP アドレスを設定時に管理 IP アドレスが不明になった場合にリカバリは必要となります。
リカバリを実行することにより、管理 IP アドレスを消去します。

No 2.2.2 リカバリを実行すると、設定された構成プロファイルは消去されてしまいますか？

回答：いいえ。SSH と HTTPS のアクセス・ルール以外の構成プロファイル(VPN, ファイヤーウォール, パスワード等)は、消去されません。

2.3 Flash Procedure

No 2.3.1 フラッシングは、どういう状況で行なうのでしょうか？

回答：パスワードが不明な状況の場合にフラッシングを行なう必要があります。
フラッシングは、構成プロファイルの全てを消去してしまいますので、注意が必要です。
(アンチウイルス・ライセンスも消去されますので、再インストールが必要となります)

No 2.3.2 フラッシングの手順を教えてください。

回答：アルテック・エーディエス e-セキュリティ事業部のホームページの mGuard 設定例 リカバリを参照してください。 <http://www.e-security-ads.com>

No 2.3.3 Windows TFTP/DHCP サーバに関する問題

回答：クライアント PC の IP アドレスを変更した場合、以下のステップを必要とします。
TFTP サーバを起動します。エラーメッセージが表示されますので、無視します
<Settings> をクリックして、次に <OK>.をクリックします。
TFTP サーバを Restart します。

No 2.3.4 DHCP サーバが IP アドレスを送った後に中央 LED は赤く点灯します。

回答：ファームウェアファイルが保存しているフォルダと TFTP サーバのアップデート・ディレクトリで指定しているフォルダが同じフォルダになっていることを確認してください。

No 2.3.5 以下のエラーメッセージが表示されます。

“ The system cannot find the file specified (rollout.sh) “

回答：rollout.sh ファイルを設定されていない場合は、このエラーメッセージを無視してください。

3 VPN

3.1 General Questions

No 3.1.1 10 VPN トンネル とは？VPN トンネル数ですか又 IP のコネクション数ですか？

回答： IP のコネクション数ではなく、mGuard で構成することができる VPN トンネルの最大数です。

No 3.1.2 事前共有鍵シークレット(PSK)を使用できる状況は？

回答： 両方の機器にスタティック IP アドレスを設定していること。

又は、ダイナミック IP アドレスで DynDNS サービスを使用している場合。

VPN を接続使用している機器の間に NAT 機能の機器が設置されている場合は、事前共有鍵シークレット (PSK) では、接続できません。X.509 証明書 (RSA) が必要となります。

No 3.1.3 Dead Peer Detection(DPD)とは？

回答： Dead Peer Detection を構成するために 3 つのパラメータがあります。

Delay (遅延)、タイムアウト、動作の 3 つです。

デフォルトで、タイムアウト=120、動作 = Hold、Delay (遅延) = 30 になっています。

VPN トンネル上に通信が 30 秒間の間、無通信の場合、mGuard はリモート機器の有効性を確認する為に DPD Keep Alive Query HELLO (R_U THERE) をリモート機器に送信します。

リモート機器が 120 秒以内に Keep Alive Query に答えないと、mGuard はリモート機器が死んでいると判断します。

正常の場合は、リモート機器から ACK (R-U-THERE-ACK) が返答してきます。

No 3.1.4 両方の mGuardn の間に NAT ゲートウェイが設置されている場合、どうい設定が必要でしょうか？

回答： 以下の設定が必要となります。

どちらかの mGuard のみ「*へ接続開始」を選択します。もう片方の mGuard は、「*から接続を待つ」に設定をします。(mGuard メニュー -> VPN -> 接続スタートアップの項目)

証明方法として、X.509 証明書を使用します。

mGuard の設定で、リモート側の VPN ゲートウェイ・アドレスの項目で、” %any “ を設定してください。NAT ゲートウェイの設定でポートフォワーディング機能にて UDP:500 と UDP:4500 を設定する必要があります。

3.2 VPN Tunnel Problems

No 3.2.1 DynDNS を使用して VPN トンネルを設定する時に、確立することができません。

またはしばらくして、失敗します。

回答: mGuard メニュー -> サービス -> DynDNS 監視項目にて、確認をしてください。

No 3.2.2 DynDNS を使用する VPN トンネルが 2、3 時間後に中断されます。

回答: mGuard メニュー -> サービス -> DynDNS 監視項目にて、確認をしてください。

No 3.2.3 VPN トンネルが確立できましたが、片方向しか通信ができません。

回答: クライアント PC のデフォルト・ゲートウェイアドレスが、mGuard の内部 IP アドレスを指定されていることを確認してください。

No 3.2.4 VPN トンネルを確立することができません。理由は何でしょうか?

回答: VPN トンネルはフェーズ 1 (ISAKMP) / フェーズ 2 (IPsec) にて確立されます。

フェーズ 1(ISAKMP)が確立されない場合

お互いの機器の事前共通鍵(PSK)か X.509 証明書(RSA)が、間違っている。

ISAKMP ポリシー設定が間違っている。お互いの機器の設定を比較してください。

フェーズ 1(ISAKMP)は確立されますが、フェーズ 2(IPsec)が確立されません。

IPsec ポリシー設定が間違っている。お互いの機器の設定を比較してください。

トンネル設定を確認してください。ローカルネットワークとリモートネットワークとは、別のネットワークにしてください。

No 3.2.5 VPN 接続を確立することができません。また、ipsec daemon は始動されません。

回答: mGuard メニュー -> アクセス -> パスワードの項目を確認してください。

設定している場合は、Web ページにアクセスしようとする、ログイン画面が表示されます。

ログイン後、VPN は確立できます。

No 3.2.6 以下のメッセージが表示されました。

“cannot initiate connection without knowing peer IP address “

回答：事前共通鍵(PSK)を使用していて、VPN ゲートウェイのアドレスとして、” %any” が使用されている場合に、このエラーメッセージが表示されます。

PSK を使用するときは、リモートゲートウェイの IP アドレスか DynDNS を設定する必要があります。

4 Firewall

No 4.1 ファイヤーウォールの設定をする時に必要なことを教えてください。

回答： ファイヤーウォール・ルールの上から順番にチェックしていきます。

受信/送信したパケットとルールがマッチするとその下のルールはチェックされません。

プロトコルの項目に UDP 及び TCP が設定されている場合のみ From Port と To Port の項目が有効となります。

No 4.2 インカミング・ルール設定は必要でしょうか？

回答： リモートからアクセスを必要としている場合は、インカミング・ルールの設定が必要となります。

また、mGuard はステートフルインスペクションを採用していますので、内側から通信を確立した場合は、インカミング・ルールの設定に関わらず、パケットを内側に入れます。

No 4.3 インターネットへのアクセスを防ぎたいと思いますが、正常に動作をしません。

回答： インターネットへのアクセスを防ぐ場合は、以下のように設定します。

プロトコル=TCP、From Port=any 、 To Port=80 を指定してください。

No 4.4 クライアント PC から mGuard までの ICMP Echo Request は、ファイヤーウォールのログに表示されません。

回答： ICMP パケットがファイヤーウォールを通過していないので、この動作は正常です。

No 4.5 ファイヤーウォールのインカミング設定で全て「拒否」の設定の時にポートフォワーディングで、クライアント PC に対して通信ができてしまう。

回答： この動作は正常です。ポートフォワーディング機能はファイヤーウォールより高い優先度があります。

従って、ポートフォワーディングが有効となるパケットに対しては、ファイヤーウォールを通過します。

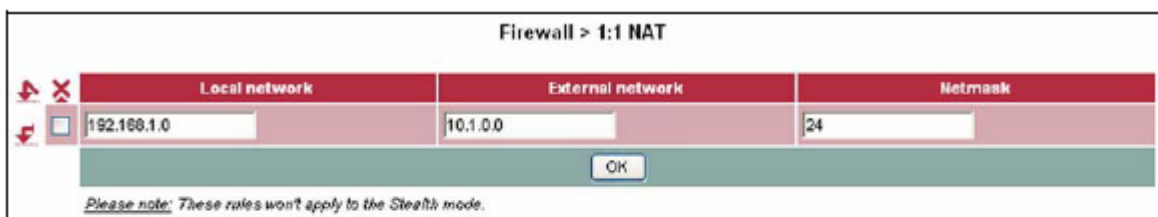
No 4.6 MAC フィルタの設定にて一定の PC からのみ通信を許可にしたが、設定していない PC からも通信ができてしまう。

回答：MAC フィルタ・ルールの場合は、ファイヤーウォール・ルールと異なって、ルールを定義していない状態で、全て「許可」になっています。従って、アクセスを拒否にする必要がある場合は、ルールが一番下に以下のルールを追加しますと、「許可」のルール以外のパケットについては「拒否」となります。

Source MAC = xx:xx:xx:xx:xx:xx Destination MAC = xx:xx:xx:xx:xx:xx Ethernet protocol = IPv4 Action = Drop

No 4.7 1:1NAT は、どういう状況で使用するのでしょうか？

回答：1:1 NAT は内部のネットワークから外部のネットワークまでアドレスを反映します。指定されたネットマスクによって、IP アドレスのホストアドレス・フィールドは変更なく維持します。以下の例では、mGuard はルータ・モードとして動作し、ネットワーク 192.168.1.0/24 (内部)と 10.1.0.0./16 (外部) 間に設置します。

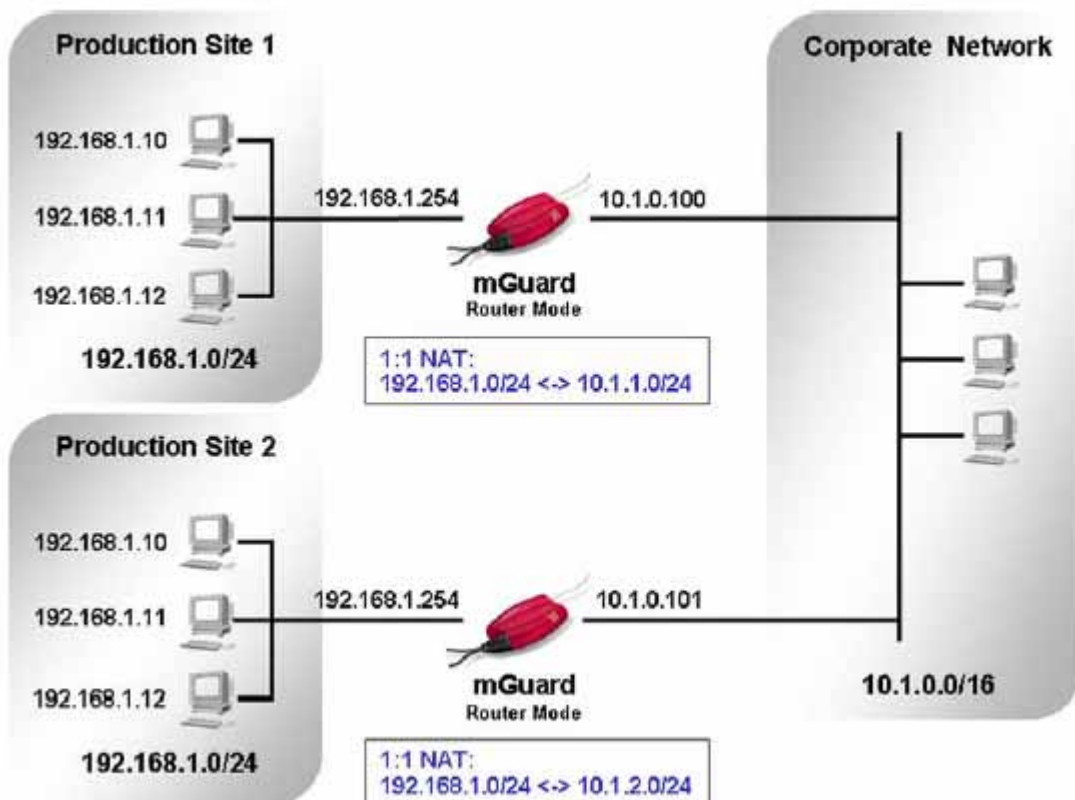


Masquerading:

192.168.1.27 <-> 10.1.0.27
 192.168.1.28 <-> 10.1.0.28
 192.168.1.29 <-> 10.1.0.29
 192.168.1.30 <-> 10.1.0.30

上記の様に Source IP アドレスが変換されます。

以下の例では、2つのエリア[Production Site](同じネットワーク IP:192.168.1.0/24 を使用)がネットワーク IP:10.1.0.0/16 で Corporate Network に接続できます。
 1:1 NAT を使用する利点とは、ルートを追加した場合に Corporate Network の定義の変更は必要ありません。
 企業のネットワークで、エリアを追加される場合に最適です。
 また、Corporate Site から Production Site へアクセスする事も可能です。



No 4.8 ファイヤーウォールのスループットが不十分

回答: mGuard メニュー -> ネットワーク -> MAU 構成 を確認してください。

LAN カード MAU 設定と mGuard の MAU 設定を同じにしてください。

インターフェースについて(FDX=全二重、HDX=半二重)

クライアント PC の LAN カードがオートネゴシネーションに対応していない場合、mGuard の MAU 構成にて FDX 固定 / HDX 固定 に設定する必要があります。

例えば、クライアント PC の LAN カードの設定が、FDX 固定で mGuard の設定が

オートネゴシネーションの場合は、オートネゴシネーションで情報が得られないので、安全な HDX に設定してしまいます。この場合、スループットは減少します。

5 Services

No 5.1 NTP サーバを設定して、NTP サービスを可能にしましたが、正常に動作をしません。

回答: mGuard の DNS 設定を確認してください。 mGuard メニュー -> サービス -> DNS

No 5.2 DHCP リレーに関する問題

回答: DHCP リレーを設定する時に、以下のポイントに注意をしてください。

mGuard の外部インターフェースにスタティック IP アドレスが必要となります。

DHCP サーバのルートに mGuard の内部ネットワークを追加する必要があります。

6 Anti Virus Protection (AVP)

No 6.1 アンチウイルスのライセンスについて教えてください。

回答： アンチウイルス・ライセンスを購入すると、販売代理店から、次の2つの情報が送られてきます。

Voucher Serial Number

Voucher Key

mGuard メニュー -> アンチウイルス -> ライセンス取得画面で必要な情報を入力します。

1~2日後に、メールでライセンスが送られてきます。

mGuard メニュー -> アンチウイルス -> ライセンス・インストールでライセンスをインストールします。これで、アンチウイルス機能が動作しています。

詳細は、アルテック・エーディエス e-セキュリティ事業部のホームページの mGuard 設定例 アンチウイルスを参照してください。 <http://www.e-security-ads.com>

No 6.2 mGuard で「5Mbyte 以上ブロックする」の設定の時に添付ファイル:5Mbyte 以上を受信した場合スキャンすることができないので、その後のメールが受信できなくなる。

回答： この問題はメールクライアントによって発生しています。

受信できなかったメールは、その後のメールの受信の妨げになります。(メールクライアントによって異なります)

mGuard で、スキャンのファイル・サイズを制限した場合は、メールクライアントのセットアップを変更してメールのヘッダラインだけを受信するようにしてください。

(詳細につきましては、お使いのメール・クライアントの説明書をお読み下さい)

No 6.3 AVP データベースをアップデートするときの問題

回答： 以下のメッセージが表示されている場合

Error messages in Anti-Virus -> Update Logs: Trying to update from server

http://anonymous:anonymous@downloads.kav.innominate.com/bases/arm_set/ FATAL ERROR:

AVP データベースサーバが見つからない為、アップデートをすることができませんでした。

この場合、以下の項目を確認してください。

mGuard メニュー -> サービス -> DNS で、DNS を確認してください。

クライアント PC で、ファイヤーウォールが設定されている場合、ICMP Echo Request を許可に設定をしてください。

7 Third Party Products

No 7.1 ステルス・モードで使用 : TFTP を使用したシスコの機器のファーム・アップができません。

回答: シスコの機器のファーム・アップはシスコの機器から開始されます。

従って、mGuard のファイヤーウォール (インカミング) の設定で、UDP : 69 「許可」 に設定する必要があります。

No 7.2 mGuard は、IPX をサポートしていますか？

回答: いいえ。mGuard は、IP/IPX をサポートしていません。

しかし、MAC フィルタを使用して、IPX フレームを制御することはできます。