リモートアクセス on Cisco ESA/WSA/SMA のための FAQ の Technote

目次

概要

この資料は Cisco テクニカル サポート コンテンツ セキュリティ アプライアンス モデルによってリモートアクセスの使用についての FAQ に対する回答を on Cisco 提供したものです。 これには Cisco E メール セキュリティ アプライアンス（ESA）、Cisco Web セキュリティ アプライアンス（WSA）、および Ciscoセキュリティ 管理 アプライアンス（SMA）が含まれています。

前提条件

使用するコンポーネント

この文書に記載されている情報は AsyncOS のバージョンを実行する Cisco コンテンツ セキュリティ アプライアンス モデルに基づいています。

リモートアクセスとは何か。

リモートアクセスは Cisco コンテンツ セキュリティ アプライアンス モデルから Cisco のセキュア ホストへの有効に なる セキュア シェル（SSH）接続です。 リモート セッションが有効に なれば Ciscoカスタマー 支援だけアプライアンスにアクセスできます。 リモートアクセスは Ciscoカスタマー カスタマ· サポートがアプライアンスを分析するようにします。 サポートはこ

のプロシージャがアプライアンスと upgrades.ironport.com サーバの間で作成する SSH トンネルによってアプライアンスをアクセス しました。

リモートアクセスがどのようにはたらくか

リモートアクセス接続 開始が、アプライアンス セキュアを、ランダム開く時、1 設定される/次の Cisco コンテンツ セキュリティサーバの選択されたポートへのアプライアンスの SSH 接続による高出典 ポート:

IP アドレス	[hostname]	使用目的
63.251.108.107	upgrades.ironport.com	すべてはセキュリティ アプライアンス モデルを満足させます
63.251.108.107	c.tunnels.ironport.com	Cシリーズ アプライアンス (ESA)
63.251.108.107	x.tunnels.ironport.com	X シリーズ アプライアンス (ESA)
63.251.108.107	m.tunnels.ironport.com	M シリーズ アプライアンス (SMA)
63.251.108.107	s.tunnels.ironport.com	S シリーズ アプライアンス (WSA)

上で許可するために顧客 ファイアウォールがリスト サーバの 1 つにアウトバウンド接続を設定される必要がある場合もあることに注意することは重要です。 ファイアウォールに有効に なる SMTP プロトコル インスペクションがある場合トンネルは確立しません。 Cisco がリモートアクセスのためのアプライアンスからの接続を許可することポートは次のとおりです:

- 22
- 25 （デフォルト）
- 53
- 80
- 443
- 4766

リモートアクセス接続はホスト名とないハードコードされた IP アドレスになされます。 これは Domain Name Server （DNS）がアウトバウンド接続を確立するためにアプライアンスで設定されるように要求します。

カスタマーネットワークで、いくつかのプロトコル指向 ネットワークデバイスはプロトコル/ポート ミスマッチによるこの接続をブロックするかもしれません。 Simple Mail Transport Protocol （SMTP）はまた-わかっているデバイス接続を割り込むかもしれません。 ブロックされるアウトバウンド接続またはプロトコル指向 デバイスがあれば、デフォルト（25）以外のポートの使用が必要となるかもしれません。 トンネルのリモート エンドへのアクセスは Ciscoカスタマー カスタマ・サポートだけに制限 されます。 アプライアンスのためのリモートアクセス接続を確立するか、または解決することを試みた場合アウトバウンド接続のためのファイアウォール/ネットワークを検討することを確かめて下さい。

> **注:** Ciscoカスタマー サポートエンジニアがリモートアクセスによってアプライアンスに接続されるときアプライアンスのシステム プロンプトは示します *(サービス)* 。

リモートアクセスをイネーブルにする方法

> **注:** アプライアンスのユーザガイドおよび「Cisco テクニカルサポート担当者のためのリモートアクセスを」有効に することに関する説明に関しては AsyncOS のバージョンを検討すること確実でであって下さい。

> **注:** 電子メールで送信 される attach@cisco.com への添付ファイルはセキュア送信中ではないかもしれません。 サポート ケース マネージャはケースに情報をアップロードする Cisco の好まれたセキュア な オプションです。 詳細を他のファイル アップロード オプションのセキュリティおよびサイズ制限について学ぶため: Cisco Technical Assistance Center への顧客 ファイル アップロード

インターネットから達することができるポートを識別して下さい。 デフォルトは電子メール メッセージを送信 するためにシステムはまたそのポート上の一般のアクセスが要求するのでほとんどの環境ではたらくポート 25 です。 このポート上の接続はほとんどのファイアウォール構成で許可されます。

CLI

CLI によってリモートアクセス接続を、管理者ユーザのような確立することは、これらのステップを完了します:

1. **techsupport** コマンドを入力して下さい
2. **トンネルを**選択して下さい
3. ランダム シードする ストリングを生成するか、または*入力すること*を選択して下さい
4. 接続のためのポート番号を規定 して下さい
5. サービス アクセスをイネーブルにするために「**Y**」を答えて下さい

リモートアクセス wil は現時点で有効に なります。 アプライアンスは今 Cisco でセキュア要塞ホストに信頼できる接続を確立するためにはたらきます。 アプライアンス シリアル番号をおよびケースをサポートしている TAC エンジニアに生成されるシードする ストリングを両方提供します。

GUI

GUI によってリモートアクセス接続を、管理者ユーザのような確立することは、これらのステップを完了します:

1. **助けるべき**ナビゲート**およびサポート > リモートアクセス**（ESA、SMA のために）、**サポートおよびヘルプ > リモートアクセス**（WSA のために）
2. 『Enable』 をクリック して下さい
3. シードする ストリングのための方式を選択して下さい
4. *セキュアトンネル* チェックボックスで*開始接続*をチェックし、接続のためのポート番号を規定 するようにして下さい
5. [Submit] をクリックします。

リモートアクセス wil は現時点で有効に なります。 アプライアンスは今 Cisco でセキュア要塞ホストに信頼できる接続を確立するためにはたらきます。 アプライアンス シリアル番号をおよびケースをサポートしている TAC エンジニアに生成されるシードする ストリングを両方提供します。

リモートアクセスをディセーブルにする方法

CLI

1. **techsupport** コマンドを入力して下さい

2. 『Disable』 を選択 して下さい
3. 本当にか」。サービス アクセスをディセーブルにしたいと思うプロンプト表示された場合 「「Y」を答えて下さい

GUI

1. **助けるべき**ナビゲート**およびサポート > リモートアクセス** (ESA、SMA のために)、**サポートおよびヘルプ > リモートアクセス** (WSA のために)。
2. 『Disable』 をクリック して下さい
3. GUI 出力は「成功示したもので—リモートアクセスはディセーブルにされました」を

リモートアクセス 接続をテストする方法

アプライアンスからの Cisco への接続のための最初のテストを行うためにこの例を使用して下さい:

```
example.run> > telnet upgrades.ironport.com 25

Trying 63.251.108.107...
Connected to 63.251.108.107.
Escape character is '^]'.
SSH-2.0-OpenSSH_6.2 CiscoTunnels1
```

接続は上記リストに記載されているポートの何れかのためにテストすることができます: 22、25、53、80、443、か 4766。 接続が失敗した場合、接続がアプライアンス/ネットワークからどこに失敗しているか見るためにパケットキャプチャを実行する必要がある場合もあります。

リモートアクセスが SMA で動作しない理由

リモートアクセスは SMA で SMA がインターネットへのダイレクトアクセスなしにローカルネットワークに置かれる場合有効に ならないかもしれません。 この例の場合、リモートアクセスは ESA か WSA で有効に し SSH アクセスは SMA で有効に することができます。 次にこれは ESA/WSA に、および SSH によって ESA/WSA から SMA にリモートアクセスによって最初にに Ciscoサポートを接続します可能にします。 これはポート 22 の ESA/WSA と SMA 間の接続を必要とします。

> **注:** アプライアンスのユーザガイドおよび「直接インターネット接続のないアプライアンスへのリモートアクセスを」有効に することに関する説明に関しては AsyncOS のバージョンを検討すること確実でであって下さい。

CLI

CLI によってリモートアクセス接続を、管理者ユーザのような確立することは、これらのステップを完了します:

1. **techsupport** コマンドを入力して下さい
2. **SSHACCESS を**選択して下さい
3. ランダム シードする ストリングを生成するか、または*入力することを*選択して下さい

4. サービス アクセスをイネーブルにするために「Y」を答えて下さい

リモートアクセス wil は現時点で有効に なります。 CLI 出力はシードする ストリングを示したものです。 Ciscoカスタマー サポートエンジニアにこれを提供して下さい。 CLI 出力はまたアプライアンス シリアル番号を含む接続ステータスおよびリモートアクセス 詳細を、示したものです。 顧客 カスタマーサポートエンジニアにこのシリアル番号を提供して下さい。

GUI

GUI によってリモートアクセス接続を、管理者ユーザのような確立することは、これらのステップを完了します:

1. **助けるべき**ナビゲート**およびサポート > リモートアクセス**（ESA、SMA のために）、**サポートおよびヘルプ > リモートアクセス**（WSA のために）
2. 『Enable』 をクリック して下さい
3. シードする ストリングのための方式を選択して下さい
4. *セキュアトンネル* チェックボックス*で開始接続*をチェックしないで下さい
5. [Submit] をクリックします。

リモートアクセス wil は現時点で有効に なります。 GUI 出力は成功 メッセージおよびアプライアンスのシードする ストリングを示したものです。 Ciscoカスタマー サポートエンジニアにこれを提供して下さい。 GUI 出力はまたアプライアンス シリアル番号を含む接続ステータスおよびリモートアクセス 詳細を、示したものです。 顧客 カスタマーサポートエンジニアにこのシリアル番号を提供して下さい。

SSHACCESS のために有効に された場合リモートアクセスをディセーブルにする方法

SSHACCESS のためのリモートアクセスをディセーブルにすることは上でそのまま同じステップです。

トラブルシューティング

アプライアンスが有能ではないイネーブルになったリモートアクセスでし、upgrades.ironport.com にリストされているポートの 1 つによって接続する場合アウトバウンド接続は失敗しますものにより検討するためにアプライアンスからパケットキャプチャを直接実行する必要があります。

> **注:** アプライアンスのユーザガイドおよび「パケットキャプチャ」の実行に関する説明に関しては AsyncOS のバージョンを検討すること確実でであって下さい。

Ciscoカスタマー サポートエンジニアは .pcap ファイルをトラブルシューティングと検討し、助けるために提供してもらうように要求するかもしれません。

関連情報

- ESA に関する FAQ： ESA で使用できる管理者アクセスのレベルは何ですか。
- Cisco E メール セキュリティ アプライアンス 製品サポート
- Cisco Web セキュリティ 製品サポート

- Cisco コンテンツ セキュリティ管理アプライアンス 製品サポート
- テクニカルサポートとドキュメント - Cisco Systems