Bastionne's Secure Digital Interaction Technology: Your Guide to Optimized Cloud Security

日本語

導入

セキュアなデジタルインタラクションの未来へようこそ。デジタル接続が必要不可欠なものとなった現代において、クラウドコンピューティング、ネットワーキング、制御システムのセキュリティは非常に重要です。広く使用されている伝統的なインフラとプロトコルには、本質的な脆弱性があり、組織をサイバー脅威に晒し、運営の完全性と企業の評判を危険にさらしています。

このような状況において、Bastionneのセキュアデジタルインタラクション（SDi）技術は画期的な進歩を示しています。SDiを採用することで、導入が容易で管理しやすいシステムを選ぶだけでなく、企業のネットワークやデバイスをサイバー脅威から保護することを確実にします。これは、今日のデジタル駆動の風景における予防セキュリティの最高峰を象徴しています。

BastionneのSDi技術を選んでいただき、ありがとうございます。このガイドは、クラウドネットワーキングの経験がある個人を対象にしており、基本的なセットアップで当社の技術を実装するための包括的なステップバイステップのマニュアルを提供します。デジタルインタラクションのセキュリティを高めることへの関心は称賛に値し、私たちはあなたを全力でサポートします。

クラウドベースのソリューションでは、2台のVMか、クラウドVMと物理的なコンピュータが必要です。1台のVMはクラウドネットワーク（vNet、VPCなど）に配置し、もう1台のVMはクラウドネットワークに接続するエンドポイントの前に配置します。エンドポイントマシン/VMは小さいもので十分で、ほとんどの使用例では1-4GBのメモリが適しています。これらのマシンはガードノードとして機能し、クラウドネットワークに接続する各アセットやデバイスの前に理想的に配置することで、クラウドネットワークを完全に保護します。

クラウドネットワークにおけるSDiセットアップ クラウドベンダーで新しいVMを作成

1. クラウド管理ページで、一般的な用途またはコンピュート最適化されたVMを選択します。

- オペレーティングシステムとしてLinux Ubuntuを選択します。
- 約1000台のデバイスを異なる地域で使用する場合、またはテキスト中心のコンテンツの場合は、およそ4GBのメモリを備えたVMを選択します。
- ローカライズされたエンドポイントやデータ重視のコンテンツ（ビデオなど）に対応する場合は、8GBのVMを選択します。より大規模な運用、例えば最大10,000台のエンドポイントを管理する場合は、16-32GBのメモリと少なくとも4つのvCPUを備えたVMを選択します。保護するデータの種類に基づいて調整します。より多くの接続に対応するためには、追加のSDiゲートウェイを展開します。
- VMにはSSDストレージを選択します。受け取る接続量に基づいてストレージをスケールしますが、ほとんどの使用例では2-5GBの空き容量で十分です。
- 保護したいデバイスと同じネットワーク（vNet、VPCなど）にこのVMを配置します。VMに公開IPアドレスが割り当てられていることを確認してください。
- ロードバランサーを使用する場合は、セッションの持続性とエンドツーエンドの暗号化に対応していることを確認してください。

2. クラウドネットワークのセキュリティ設定を構成

- 管理ページからVMのネットワークセキュリティ設定に移動し、TCPデータの受信用ポート（例：8080）を指定します。これが他のSDiゲートウェイからデータを受信する場所になります。
- （オプション）特定のIPに対する受信アクセスを制限したい場合は、リモートで接続するIPや他のSDiゲートウェイのIPを指定します。これは厳密には必要ではありません。SDiゲートウェイには組み込みのホワイトリスト機構があります。

3. クラウドベンダーのマーケットプレイスからSDiをダウンロード

- 新しく展開されたVMで、SDiページのマーケットプレイスの指示に従って、ソフトウェアをVMにダウンロードします。

4. SDiゲートウェイの設定

- SDiがインストールされたVMで、端末を開いて「screen」と入力し、Enterキーを押します。screenがインストールされていない場合は、「sudo apt-get install screen」と入力してインストールできます。
- SDi実行ファイルが保存されている場所に移動し、「sudo ./BastionneBox」と入力して実行します。

- 256ビットの暗号化キーを生成するか、入力するように求められます。このキーを安全に保管し、バックアップを取ります。キーが侵害されたり失われたりした場合、ゲートウェイとその上のすべてのデータをリセットする必要があります。
- ここから、SDiゲートウェイを緩いモードかロックダウンモードで実行するかを尋ねられます。高いセキュリティが必要な場合はロックダウンを選択します。これにより、非認可のエンドポイント（つまり、SDiゲートウェイで保護されていないエンドポイント）への接続が完全に遮断されます。8つのオプションが表示されます。「4」と入力してEnterキーを押し、接続を設定します。同じクラウドネットワーク（vNet、VPCなど）上にある、保護したいデバイスのプライベートIPアドレスを入力します。
- 保護したい他のデバイスのパブリックIPアドレス、つまり目的のIPアドレスを入力します。
- 他のSDiゲートウェイのパブリックIPアドレスを入力します。先に入力したIPと同じでも構いませんが、異なるパブリックIPを持っている場合は適切に入力します。
- ステップ2（クラウドネットワークの設定を構成）で指定したポートを入力します。
- この設定をサーバーモードで実行するかどうかを選択します：他のSDiゲートウェイがリモートユーザーの保護に使用される場合は、このゲートウェイでサーバーモードを選択します。他のゲートウェイが外部リソース（サーバーなど）の保護に使用される場合は、「no」と入力します。

5. ソブリン**MIM**コードの生成

- ここで、設定用のMIMコードを生成できます。「2」と入力し、前のステップで追加した設定を選択します。そのインデックスは「0」です。
- 生成されたコードをコピーして、後で使用するために安全な方法で保管します。

6. SDiゲートウェイの起動

- ステップ4（SDiゲートウェイの設定）でサーバーモードを選択した場合、この時点で「3」と入力してゲートウェイを起動できます。
- ステップ4でサーバーモードを指定しなかった場合は、他のSDiゲートウェイをまず設定し、サーバーモードに指定してから起動する必要があります。その後、このユニットを起動できます。
- ゲートウェイを起動した後、Ctrl-Aを押してからDを押すことでスクリーンセッションから切り離します。VMセッションを閉じることが

他のデバイス用SDiセットアップ

1. 指定されたLinux（Ubuntu）マシンにSDiをダウンロードしてインストールします。

- このデバイスはVMまたは物理コンピュータのいずれかであることができます。
- このデバイスが同じネットワーク上の複数のデバイスへのアクセスを保護するために用いられる場合は、クラウドSDiユニットと同様のサイズ推奨事項に従ってください。
- ただし、ターゲットデバイス（つまり、クラウド内の非SDiマシン）に接続する各クライアントデバイスは、理想的には独自のSDiユニットを持っているべきです。これにより、セキュリティが強化され、より小さなデバイスでもSDiを収容できます。
- 例えば、1～4GBのメモリを持つシングルボードコンピュータやマイクロPCでほとんどのタスクに十分です。
- https://www.bastionne.com/sdi/download にアクセスしてダウンロードするか、指定されたマシンの端末で「curl -O https:// www.bastionne.com/sdi/download/BastionneBox」を実行します。
- ターゲットデバイスが同じネットワーク上でこのマシンにイントラネット経由でアクセスできることを確認してください。理想的には、ターゲットデバイスでイーサネットケーブルを使用し、WiFiをオフにします。
- ターゲットデバイスでWiFiを使用する必要がある場合は、ターゲットデバイスのファイアウォールルールを更新して、SDiゲートウェイのプライベートIPアドレスからのみデータを許可するようにします。

2. （オプション）デバイスがクラウドネットワークやDMZなどにも存在する場合は、ネットワークセキュリティ設定を構成します。

- TCPデータの受信用にポート（例：8080）を指定します。このSDiゲートウェイは、他のSDiユニットからここでデータを受信します。
- （オプション）特定のIPに対する受信アクセスを制限したい場合は、リモートで接続するIPや他のSDiゲートウェイのIPを指定します。これは厳密には必要ではありません。SDiゲートウェイには組み込みのホワイトリスト機構があります。

3. SDiゲートウェイの設定

- SDiがインストールされたマシンで、端末を開いて「screen」と入力し、Enterキーを押します。screenがインストールされていない場合は、「sudo apt-get install screen」と入力してインストールできます。
- SDi実行ファイルが保存されている場所に移動し、「sudo ./BastionneBox」と入力して実行します。
- 256ビットの暗号化キーを生成するか、入力するように求められます。このキーを安全に保管し、バックアップを取ります。キーが侵害されたり失われたりした場合、ゲートウェイとその上のすべてのデータをリセットする必要があります。

- ここから、SDiゲートウェイを緩いモードかロックダウンモードで実行するかを尋ねられます。高いセキュリティが必要な場合はロックダウンを選択します。これにより、非認可のエンドポイント（つまり、SDiゲートウェイで保護されていないエンドポイント）への接続が完全に遮断されます。8つのオプションが表示されます。「4」と入力してEnterキーを押し、接続を設定します。同じネットワーク上の、保護したいデバイスのプライベートIPアドレスを入力します。
- 目的のIPアドレス、つまりクラウドデバイスまたはクラウド内のSDiゲートウェイのパブリックIPアドレスを入力します。
- クラウドSDiゲートウェイのパブリックIPアドレスを入力します。先に入力したIPと同じでも構いませんが、異なるパブリックIPを持っている場合は適切に入力します。重要：ステップ2のSDiクラウドセットアッププロセス（例として8080）で指定したポートを正確に入力します。
- このゲートウェイ接続を実行するモードを選択します。他のSDiゲートウェイ接続がサーバーとして設定されている場合は、クライアントでなければなりません。逆も同様です。

4. ソブリン**MIM**コードを入力

- 「1」と入力し、前のステップで追加した設定を選択します。そのインデックスは「0」になります。
- SDiクラウドセットアッププロセスのステップ5で生成したコードを入力します。

5. SDiゲートウェイの起動

- ステップ3（SDiゲートウェイの設定）でクライアントモードを選択した場合、他のゲートウェイがすでに開始されていることを確認してから、「3」と入力します。
- このゲートウェイの設定がサーバーモードとして指定されていた場合、まずこのユニットでゲートウェイを「3」と入力して起動します。
- ゲートウェイを起動した後、Ctrl-Aを押してからDを押すことでスクリーンセッションから切り離します。セッションに再度接続するには、端末で「screen -r」と入力します。

デフォルトルートの設定

1. クラウドデバイスとターゲットの両方にデフォルトルートを設定

- これらのマシンへのデータのやり取りは、今後、パケットごとにMIMトークンで暗号化され、検証されます。
- 設定に応じて、デフォルトルートを設定した後、これらのマシンへのすべてのアクセスにはSDi接続が必要になります。この点を計画に含めてください。
- 同じネットワーク上にある複数のSDiゲートウェイにデバイスを接続する場合は、先に述べたように使用する全体的なSDiゲートウェイを指定し、その後、ターゲットデバイスのファイアウォールまたはネットワーク設定を通じて使用するサブSDiゲートウェイを指定します。

これにて、クラウドと外部デバイス間のBastionneのセキュアデジタルインタラクション技術のセットアップガイドを終了します。初期セットアップのSDiクラウドゲートウェイが最も時間を要する部分ですが、その後の接続は効率と使いやすさのために効率化されています。デジタルセキュリティのニーズにBastionneを信頼していただき、ありがとうございます。