仮想アプライアンスおよびADコネクタ導入向けのセキュアなCisco Umbrella

内容

はじめに

このドキュメントでは、Cisco Umbrella仮想アプライアンス(VA)およびActive Directory(AD)コネクタの使用によって発生する内部攻撃のリスクを軽減するための導入に関するベストプラクティスと推奨事項について説明します。

VAはUbuntu Linux 20.04の強化バージョンを実行します。お客様には、設定およびトラブルシューティングの目的でのみ、制限付きアクセスが提供されます。お客様がVAに追加のソフトウェアやスクリプトを導入することはできません。

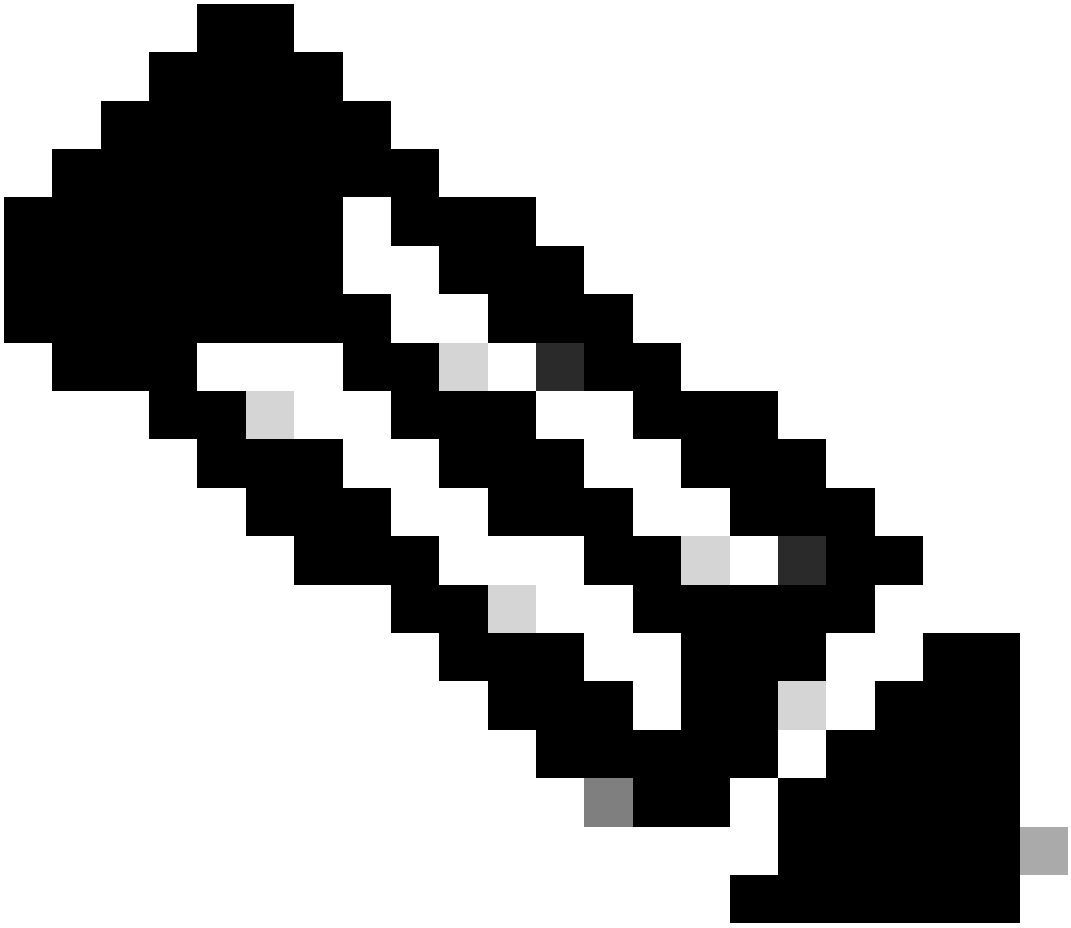
Cisco Umbrella 仮想アプライアンス

.tarファイルの管理：

- Cisco Umbrella仮想アプライアンス(VA)ソフトウェアは、実際のVAイメージとそのイメージのシグニチャを含む.tarファイルとしてUmbrellaダッシュボードからダウンロードされます。
- VAイメージの整合性を検証するためにシグニチャを検証することを推奨します。

ポートの設定：

- デフォルトでは、導入時に着信トラフィックに対して開かれているのはポート53と443だけです。
- Azure、KVM、Nutanix、AWS、またはGCPでVAを実行している場合、デフォルトではポート22も有効になっており、SSH接続でVAを設定できます。
- VMwareおよびHyper-V上で実行されているVAの場合、ポート22は、SSHを有効にするコマンドがVA上で実行されている場合にのみ開かれます。
- VAは、Umbrellaのドキュメントに記載されている宛先に対し、特定のポート/プロトコルを介して発信クエリを行います。
- Cisco Umbrellaでは、VAから他のすべての宛先へのトラフィックをブロックするルールをファイアウォールに設定することをお勧めします。



注:VAとの間のすべてのHTTPS通信は、TLS 1.2でのみ行われます。古いプロトコルは使用しません。

パスワードの管理：

- VAへの最初のログインでは、パスワードの変更が必要です。
- シスコでは、この最初のパスワード変更の後に、VA上のパスワードを定期的にローテーションすることを推奨します。

DNS攻撃の軽減：

- VA上で実行されているDNSサービスに対する内部サービス拒否攻撃のリスクを軽減するために、VA上のDNSのIPごとのレート制限を設定できます。
- これはデフォルトでは有効になっていないため、Umbrellaのドキュメントに記載されている手順に従って明示的に設定する必要があります。

SNMPでのVAのモニタリング：

- SNMPでVAを監視する場合、Cisco Umbrellaでは認証と暗号化にSNMPv3を使用することを推奨しています。
- 同じ手順については、Umbrellaのドキュメントを参照してください。
- SNMPモニタリングを有効にすると、VAのポート161が着信トラフィック用に開放されます。
- VA上のCPU、負荷、メモリなどのさまざまな属性をSNMP経由で監視できます。

Cisco ADとVAの統合を使用する方法：

- Cisco Umbrella Active Directoryとの統合でVAを使用している場合は、DHCPリース時間に合わせてVAのユーザキャッシュ期間を調整（または調整）することを推奨します。
- 「仮想アプライアンス：ユーザキャッシュ設定のチューニング」の説明を参照してください。これにより、誤ったユーザ属性のリスクが最小限に抑えられます。

監査ログの設定：

- VAは、VAで実行されたすべての構成変更の監査ログを保持します。
- Umbrellaのドキュメントの手順に従って、この監査ログのsyslogサーバへのリモートロギングを設定できます。

VAの設定：

- Umbrellaサイトごとに少なくとも2つのVAを設定する必要があります。これらの2つのVAのIPアドレスは、DNSサーバとしてエンドポイントに配布できます。
- 冗長性を高めるために、VAでエニーキャストアドレッシングを設定できます。これにより、複数のVAが1つのエニーキャストアドレスを共有できます。
- したがって、複数のVAを効果的に導入しながら、各エンドポイントにDNSサーバIPを2つだけ配布できます。いずれかのVAに障害が発生した場合、エニーキャストにより、DNSクエリが同じエニーキャストIPを共有する他のVAにルーティングされることが確認されます。
- VAでエニーキャストを設定する手順の詳細を参照してください。

Cisco Umbrella Active Directory Connectorの設定

カスタムアカウント名の作成：

- Cisco Umbrella AD Connectorのベストプラクティスの1つは、デフォルトのOpenDNS_Connectorの代わりにカスタムアカウント名を使用することです。
- このアカウントは、コネクタを展開する前に作成し、必要な権限を付与できます。
- コネクタインストールの一部としてアカウント名を指定する必要があります。

ADコネクタを使用したLDAPSの設定：

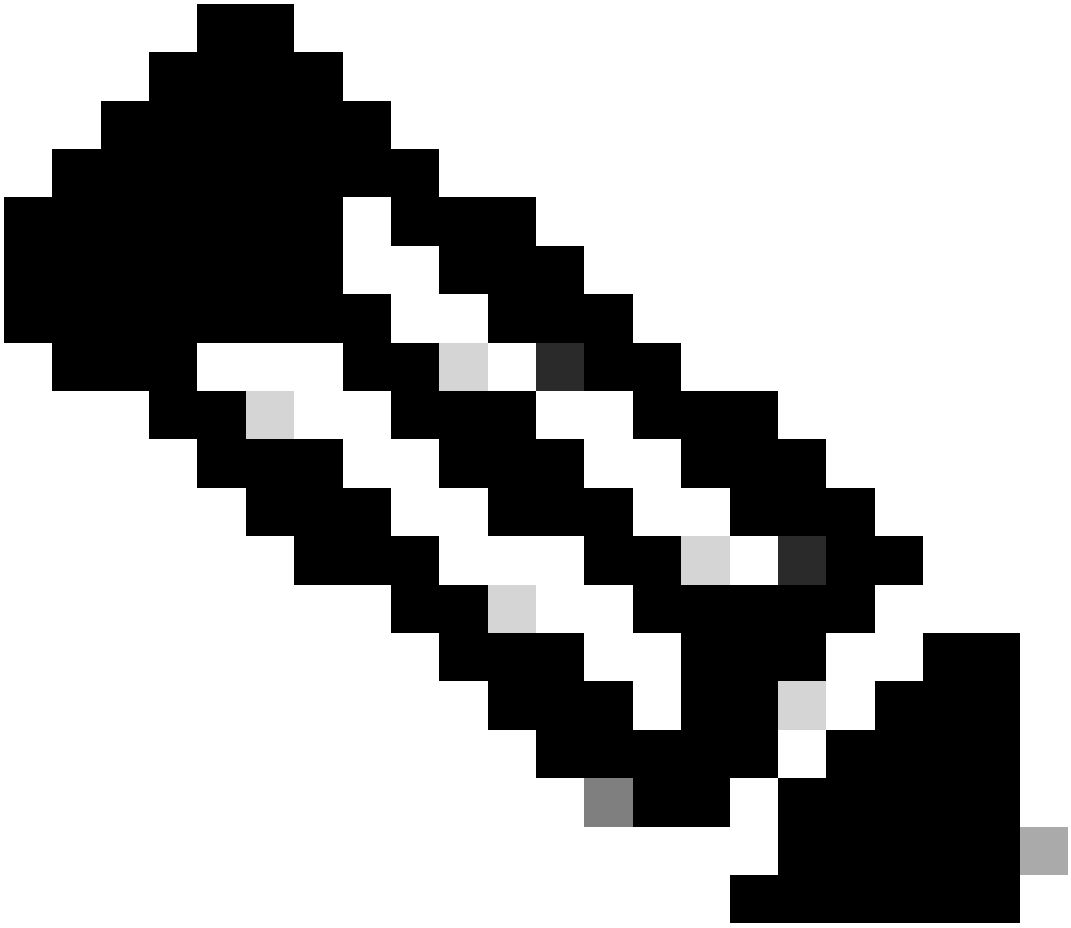
- Umbrella ADコネクタは、LDAPS（セキュアチャネル経由で送信されたデータ）経由でユーザグループ情報の取得を試みますが、失敗し、その順序でLDAP over Kerberos（パケットレベルの暗号化）またはLDAP over NTLM（認証のみ、暗号化なし）に切り替わります。
- Cisco Umbrellaでは、コネクタが暗号化チャネルを介してこの情報を取得できるように、ドメインコントローラにLDAPSを設定することを推奨しています。

.ldifファイルの管理：

- デフォルトでは、コネクタはドメインコントローラから取得したユーザとグループの詳細を.ldifファイルにローカルに保存します。
- これはプレーンテキストで保存される機密情報である可能性があるため、コネクタを実行するサーバへのアクセスを制限できます。
- または、インストール時に、.ldifファイルをローカルに保存しないように選択することもできます。

ポートの設定：

- コネクタはWindowsサービスであるため、ホストマシン上のポートは有効/無効になりません。Cisco Umbrellaでは、専用のWindowsサーバ上でCisco Umbrella AD Connectorサービスを実行することを推奨しています。
- VAと同様に、コネクタは、Umbrellaのドキュメントに記載されている宛先に対し、特定のポート/プロトコルを介して発信クエリを行います。Cisco Umbrellaでは、コネクタから他のすべての宛先へのトラフィックをブロックするルールをファイアウォールに設定することをお勧めします。



注：コネクタとの間のすべてのHTTPS通信は、TLS 1.2でのみ行われます。古いプロトコルは使用しません。

コネクタパスワードの管理：

- コネクタのパスワードは定期的に交換することをお勧めします。
- これを行うには、Active Directoryでコネクタアカウントのパスワードを変更し、コネクタフォルダの「PasswordManager」ツールを使用してパスワードを更新します。

ユーザIPマッピングの受信：

- デフォルトでは、コネクタはプライベートIPを通信します。
- ADはユーザマッピングをプレーンテキストでVAに送信します。
- このナレッジベース記事に記載されている手順に従って、暗号化チャネルを介して通信するようにVAとコネクタを設定することもできます。

証明書管理：

- 証明書の管理と失効はVAの対象外であり、お客様には、最新の証明書/証明書チェーンがVAとコネクタに適切に存在していることを確認する責任があります。
- この通信に暗号化チャネルを設定すると、VAとコネクタのパフォーマンスに影響します。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。