警告VA "；がアテンション状態である場合に解決(&Q)

内容

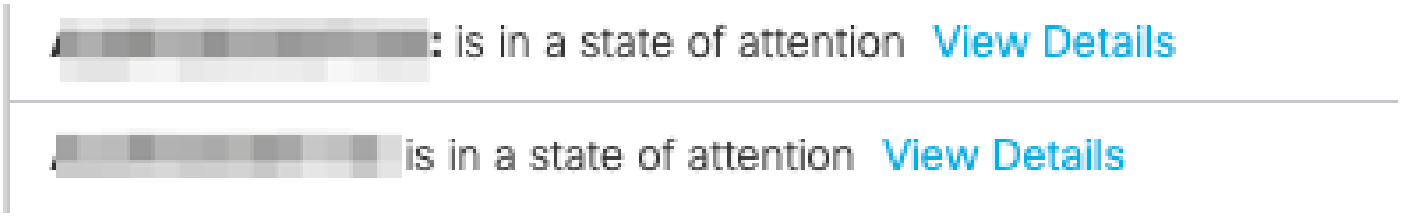
はじめに

このドキュメントでは、DNSCryptの有効化に関連して、VAが「要注意の状態にある」ことを示すVA警告を解決する方法について説明します。

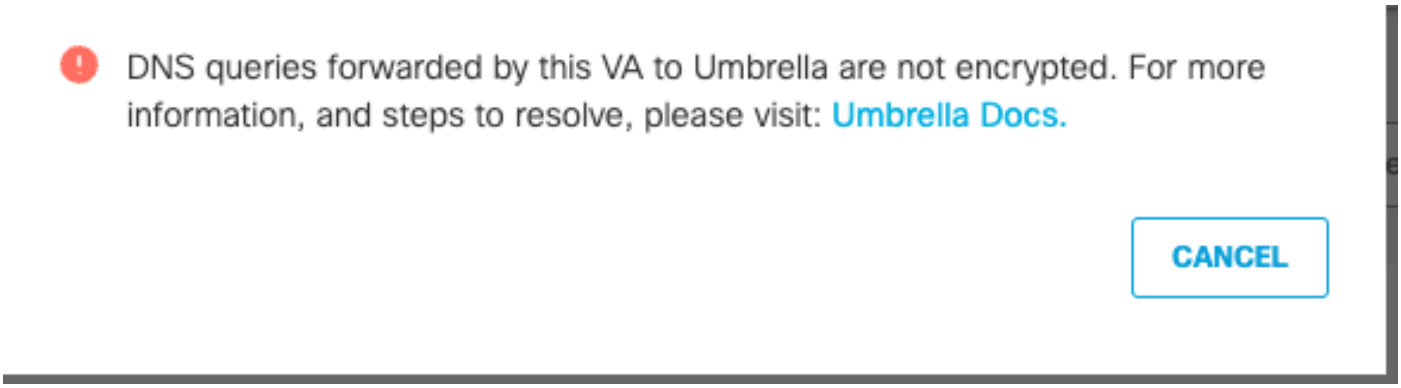
概要

仮想アプライアンス(VA)は、自身とOpenDNSパブリックドメインネームシステム(DNS)リゾルバ間のDNSCrypt暗号化をサポートします。DNSCryptは、VAが転送するDNSパケットを暗号化し、機密情報の傍受を防止します。DNSCryptは最適な保護のためにデフォルトで有効になっていますが、ファイアウォールがVAとパブリックDNSリゾルバ間の暗号化されたトラフィックをブロックする場合に問題が発生する可能性があります。

暗号化されていないDNSトラフィックは、対処が必要なセキュリティリスクです。VAとOpenDNSの間で暗号化を確立できない場合は、Umbrellaダッシュボードに、影響を受ける仮想アプライアンスが「要注意状態」であることを示す警告が表示され、可能な限り最高の保護を維持できます。



View Detailsをクリックすると、このVAによってOpenDNSに転送されたDNSクエリが暗号化されていないことを示すメッセージが表示されます。

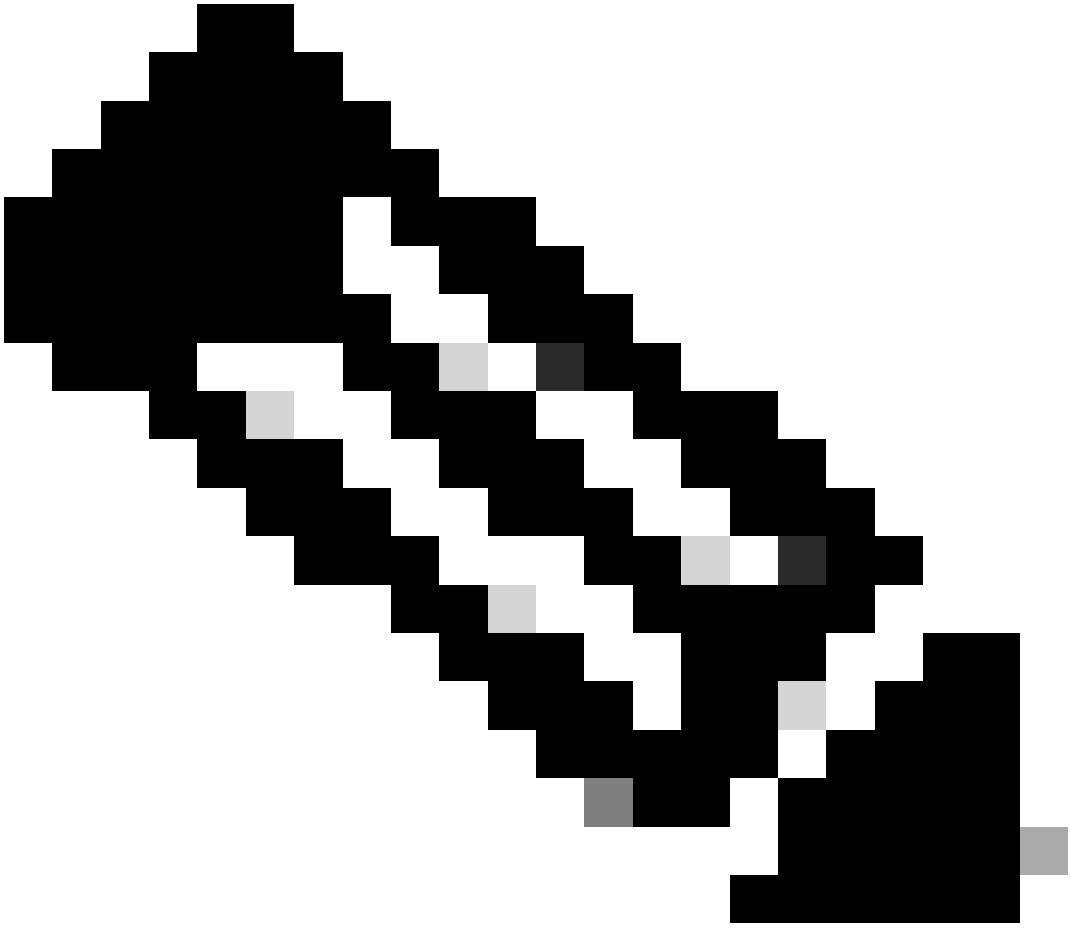


注：DNSCryptは、バージョン1.5.x以降を実行している仮想アプライアンスでのみ使用できます。VAが1つしかなく、アップグレードされていない場合、このメッセージも表示されます。

DNSCrypt警告の解決

警告を解決してDNSCrypt保護を復元するには、次の手順に従います。

1. ファイアウォールまたは侵入防御システム(IPS)/侵入検知システム(IDS)の設定を確認します。
2. ファイアウォールまたはIPS/IDSがVAに対して暗号化されたDNSCryptトラフィックを許可していることを確認します。
3. ポート53(UDP/TCP)で次のOpenDNS IPアドレスへの発信および着信トラフィックを許可します。
    - 208.67.220.220
    - 208.67.222.222
    - 208.67.222.220
    - 208.67.220.222
4. ディープパケットインスペクションでファイアウォールまたはIPS/IDSを使用する場合は、暗号化されたDNSCryptパケットをブロックまたは干渉しないことを確認します。一部のデバイスは、ポート53で標準のDNSトラフィックのみを想定している場合、これらのパケットをブロックできます。
5. 暗号化されたトラフィックが、ネットワークとパス内のすべてのデバイス上のOpenDNSリゾルバの間で発信および着信の両方を流せることを確認します。



注：ファイアウォールまたはIPS/IDSがDNSCryptトラフィックをブロックしている場合、VAの背後にいるユーザのDNS解決が失敗する可能性があります。

ファイアウォールでこのトラフィックがすでに許可されていると思われるものの警告が引き続き表示される場合は、サポートケースをオープンして、さらにサポートを求めてください。

Cisco ASAファイアウォールの動作と、ディープパケットインスペクションおよびDNSCryptに関連するエラーメッセージの可能性の詳細については、「Cisco ASAファイアウォールがUmbrella仮想アプライアンスからのDNSCrypt機能をブロックする理由」を参照してください。

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。