paloalto
TECHDOCS

高度なDNSセキュリティ管理

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

November 23, 2022

Table of Contents

DNSセキュリティ サブスクリプション サービスについて

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced DNSセキュリティ ライセンス（拡張機能サポート用）またはDNSセキュリティ ライセンス ❑ Advanced Threat PreventionまたはThreat Preventionライセンス

Palo Alto Networks®はDNSベースの脅威からの保護に特化した統合保護を提供します。、2つのセキュリティ サブスクリプション オプションがあります。DNSセキュリティとAdvanced DNSセキュリティです。これらのクラウド提供セキュリティ サブスクリプションは、包括的なDNSセキュリティ ソリューションを提供するために、Palo Alto Networksの脅威防御ソリューションとの共有基盤を使用して運用されます。そのため、Advanced Threat PreventionまたはThreat Preventionの存在が必要です。

DNSセキュリティ クラウド サービスは、多くの高度なDNSベースの脅威から組織を保護するために設計されています。DNSセキュリティは、高度な機械学習と予測分析を多様な脅威インテリジェンスソースに適用することで、強化されたDNSシグネチャを迅速に生成し、既知の悪意のあるDNSカテゴリーから防御し、DNS要求のリアルタイム解析を提供して、新しく生成された悪意のあるドメインや未知の悪意のあるドメインからネットワークを保護します。DNSセキュリティは、DNSトンネリング、DNS再バインド攻撃、自動生成を使用して作成されたドメイン、マルウェア ホストなど、多くのDNS脅威を検出できます。

サポートされているネットワーク セキュリティ プラットフォームで動作するアクティブな脅威防御ソリューションにより、お客様はPalo Alto Networksによって生成されたドメインのリストを使用してDNS要求をシンクホールすることができます。ローカルでアクセスするこれらのカスタマイズ可能な DNS シグネチャ リストはアンチウイルスおよび WildFire 更新に同梱されており、公表時点のポリシー適用および保護に最も関連する脅威が含まれています。DNS を使用する脅威をより良くカバーするために、DNS セキュリティ サブスクリプションは、ユーザーが高度な予測分析を使用してリアルタイムで保護を利用できるようにします。DGA/DNS トンネリング検出および機械学習などの技術を使用し、DNS トラフィックに潜む脅威を事前に特定し、制限なくスケーリングできるクラウドサービスで共有します。DNS シグネチャおよび保護はクラウドベースのアーキテクチャで保存されるため、様々なデータソースを使用して生成された、常に拡大するシグネチャのデータベースをフル活用できます。これによりリアルタイムで、DNS を使

用する一連の脅威、新たに生成された悪意のあるドメインを防止することができます。将来の脅威と戦うために、DNS セキュリティ サービスの分析、検出、保護機能の更新を、コンテンツ リリースを通じて利用できるようになっています。

基本的な*DNS*セキュリティ サービスにアクセスするには、ネットワーク セキュリティ プラットフォームの運用に必要な基本ライセンスに加えて、有効な*Advanced Threat Prevention*または*Threat Prevention*ライセンスと*Advanced DNS*セキュリティまたは*DNS*セキュリティ ライセンスが必要です。

DNSセキュリティ サブスクリプションは、以下のPalo Alto Networksネットワーク セキュリティ プラットフォームでご利用いただけます。

- VM-Series、CN-Seriesなどの次世代ファイアウォール
- Prisma Access

Advanced DNSセキュリティ サービスは、DNSセキュリティ サブスクリプションと連動して動作する、DNS応答の変化を検査するAdvanced DNSセキュリティ クラウドの新しいドメイン ディテクターへのアクセスを可能にし、多くの種類のDNSハイジャックをリアルタイムで検出する補完的なサブスクリプション サービスです。PAN-OS 11.2 以降のリリースで動作する Advanced DNSセキュリティにアクセスすると、乗っ取られたドメインや誤って設定されたドメインからのDNS応答を検出してブロックできます。乗っ取られたドメインや誤って設定されたドメインは、DNS応答を直接操作するか、組織のDNSインフラストラクチャの構成設定を悪用して、ユーザーを悪意のあるドメインにリダイレクトし、そこから追加の攻撃を開始することによって、ネットワークに導入される可能性があります。この2つの技術の主な違いは、エクスプロイトが発生する場所にあります。DNSハイジャックの場合、攻撃者は、DNSプロバイダーの管理アクセス、DNS解決プロセス中のMiTM攻撃、DNSサーバー自体など、組織のDNSインフラストラクチャの何らかの側面を危険にさらすことで、攻撃者が運用するドメインへのDNSクエリを解決する能力を得ます。ドメインの設定に誤りがあると、同様の問題が生じます。攻撃者は、ドメイン設定の問題を利用して、組織のDNSに自身の悪意のあるドメインを組み込むことを狙います。古いDNSレコードを使用すれば、攻撃者はお客様のサブドメインの所有権を得ることがでます。

Advanced DNSセキュリティは、クラウド ベースの検出エンジンを運用することで、乗っ取られたドメインや誤って設定されたドメインをリアルタイムで検出および分類することができます。これによりMLベースの分析情報を使用してDNS応答を分析し、悪意のある活動を検出するDNSヘルス サポートを提供します。これらのディテクターはクラウド上にあるため、ディテクターに変更が加えられたときにユーザーが更新パッケージをダウンロードしなくても、自動的に更新および展開される幅広い検出メカニズムにアクセスできます。初期リリースでは、Advanced DNSセキュリティは2つの解析エンジンをサポートしています。DNS Misconfiguration Domains (DNSの設定ミスドメイン)とHijacking Domains (ハイジャック ドメイン)です。さらに、すべてのDNSクエリに対するDNS応答がAdvanced DNSセキュリティ クラウドに送信され、応答解析が強化され、より正確に分類されて、リアルタイム交換で結果が返されます。解析モデルはコンテンツの更新によって提供されますが、既存のモデルに対する拡張機能はクラウド側の更新として実行され、ファイアウォールの更新は必要ありません。Advanced DNSセキュリティはアンチスパイウェア（またはDNSセキュリティ）プロファイルを通じて有

効化および設定され、有効なAdvanced DNSセキュリティおよびAdvanced Threat Prevention(またはThreat Prevention）ライセンスが必要です。

*Advanced DNS*セキュリティ サービスにアクセスするには、ネットワーク セキュリティ プラットフォームの運用に必要な基本ライセンスに加えて、有効な*Advanced Threat Prevnetion*または*Threat Prevention*ライセンスと*Advanced DNS*セキュリティ ライセンスが必要です。

Advanced DNSセキュリティ サブスクリプションは、以下のPalo Alto Networksネットワーク セキュリティ プラットフォームでご利用いただけます。

- VM-Series、CN-Seriesなどの次世代ファイアウォール

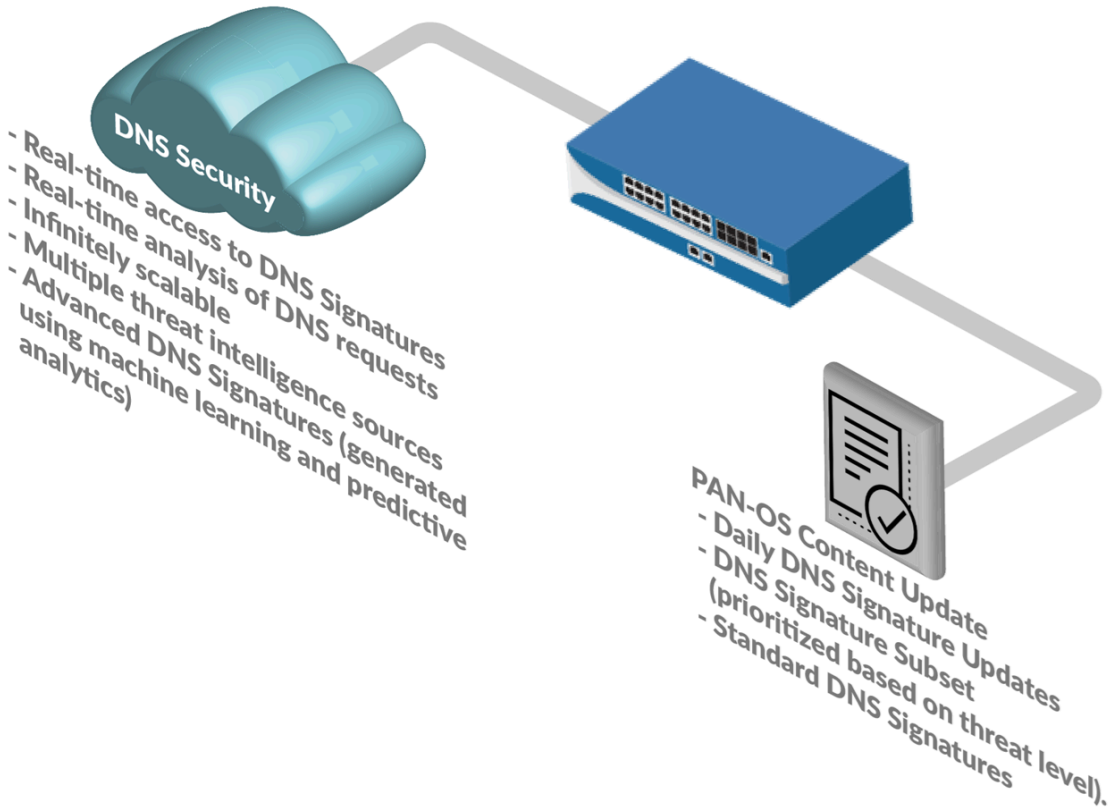
DNSセキュリティとAdvanced DNSセキュリティをネットワークにデプロイする方法をご紹介します。

- DNSセキュリティ サブスクリプション サービスの設定
- DNSセキュリティ サブスクリプション サービスの監視

クラウド配信型の DNS シグネチャおよび保護

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced DNSセキュリティ ライセンス（拡張機能サポート用）またはDNSセキュリティ ライセンス ❑ Advanced Threat PreventionまたはThreat Preventionライセンス

クラウドベースのサービスであるAdvanced DNSセキュリティとDNSセキュリティを使用すれば、制限なくスケーリングできるDNSシグネチャおよび保護ソースを利用して、悪意のあるドメインから組織を守ることができます。Palo Alto Networks が生成するドメイン シグネチャおよび保護は、WildFire トラフィック分析、パッシブ DNS、アクティブ WEB クローリングおよび悪意のある Web コンテンツ分析、URL サンドボックス分析、Honeynet、DGA リバースエンジニアリング、テレメトリーデータ、whois、Unit 42 研究組織、Cyber Threat Alliance のようなサードパーティのデータソースを元にして生成されます。オンデマンドのクラウド データベースを使用すれば、高度な分析技術を使用して生成されたシグネチャを含む Palo Alto Networks の DNS シグネチャ一式やリアルタイムの DNS リクエスト分析を利用することができます。ダウンロードしてローカルで使用できる一連の DNS シグネチャ (アンチウイルスおよび WildFire 更新に同梱) には 100,000 件のシグネチャというキャパシティ制限が規定で備わっており、高度な分析を通じて生成されたシグネチャは含まれていません。毎日のように生成される大量の新しい DNS シグネチャにより良く対応するために、クラウドベースのシグネチャ データベースが、新たに追加された DNS シグネチャをユーザーが即座に利用できるようにします。更新をダウンロードする必要はありません。ネットワーク接続がダウンした、あるいは到達できない場合、ファイアウォールはオンボックスの DNS シグネチャ セットを使用します。



DNS セキュリティ サービスは、複数の DNSデータ ソースで予測分析と機械学習を使用して、リアルタイムの DNS 要求分析を操作します。これは、DNS ベースの脅威に対する保護を生成するために使用されます。DNS ベースの脅威には、セキュリティ ポリシー ルールにアタッチされたスパイウェア対策セキュリティ プロファイルの設定を通じてリアルタイムでアクセスできます。各 DNS 脅威カテゴリ (DNS シグネチャソース) を使用すると、特定のシグネチャ タイプのログ重大度レベルだけでなく、個別のポリシー アクションを定義できます。これにより、ネットワーク セキュリティ プロトコルに応じて、脅威の性質に基づいて特定のセキュリティ ポリシーを作成できます。また、Palo Alto Networks は、PAN-DB とAlexa からのメトリックに基づいて、明示的に許可されたドメインのリストを生成および維持します。これらの許可リスト ドメインは頻繁にアクセスされ、悪意のあるコンテンツがないことが分かっています。DNS セキュリティ カテゴリと許可リストは更新され、PAN-OS コンテンツ リリースを通じて拡張可能です。

*PAN-OS 9.1*以前では、*DNS*セキュリティ ソース カテゴリーの範囲が限られています。

DNSセキュリティとAdvanced DNSセキュリティは現在、次のDNS脅威カテゴリーの検出をサポートしています:

ユニバーサル脅威*ID*番号 *(*脅威ログでは*ID*として示されます*)* は、ドメインを分類するために*DNS*によって使用される特定の*DNS*検出メカニズムにマップされます。これは、そのドメインが属する大まかな脅威のカテゴリとともに、正確なカテゴリ分けを示すものです。

- コマンドと制御ドメイン :C2 には、マルウェアや侵害されたシステムが使用する URL とドメインが含まれており、攻撃者のリモート サーバーと密かに通信して悪意のあるコマンドを受信したり、データを漏らしたり (DNS トンネリング検出や DGA 検出を含む)、またはターゲットの権限のある DNS サーバー上のリソースを枯渇させたり (NXNSattack など) します。
  - **DNS Tunnel Detection** (UTID:109001001/109001002) - DNS トンネリングは、DNS クエリと応答内の非 DNS プログラムおよびプロトコルのデータをエンコードするために攻撃者によって使用される可能性があります。これにより攻撃者は、ファイルを転送したり、システムにリモート アクセスしたりできるバック チャネルを開くことができます。DNS トンネリング検出は機械学習を使用して、ドメインの n-gram 頻度分析、エントロピー、クエリ レート、パターンなどの DNS クエリの挙動傾向を分析し、クエリが DNS トンネリング ベースの攻撃であることを示唆するかどうか判断します。これには、TriFive や Snugy など、検出を避けるために複数のドメインにわたってデータをゆっくりと浸透させる特定の次世代 DNS トンネリング マルウェアが含まれます。ファイアウォールの自動ポリシーアクションとこれを組み合わせることで、DNS トンネリングに隠されたデータ盗難や C2 を素早く検出し、定義したポリシールールに基づいて自動的にそれをブロックできるようになります。

    DNSトンネリング機能を持っていると判断されたドメインはさらに分析され、DNSクエリと応答にデータを埋め込むために使用されるツールと、DNSセキュリティによって関連付けられたマルウェア キャンペーン名の詳細が提供されます。属性の詳細は、ファイアウォールの脅威ID/名前として脅威ログに表示され、Prisma AccessのDNSセキュリティ ログは脅威名ファイアウォールとして次の形式で表示されます。Tunneling:<*optional_list_of_tools/campaigns*; dot-separated string)>:<*domain_name*>または特定のDNSトンネル ドメイン タイプに基づいてTunneling_infil:<*optional_list_of_tools/campaigns*; dot-separated string)>:<*domain_name*>
  - **DGA Domain Detection** (UTID:109000001):ドメイン生成アルゴリズム(DGA)は、ドメインを自動生成するために使用され、通常は悪意のあるコマンド アンド コントロール(C2)通信チャネルを確立するコンテキスト内で大量に生成されます。DGA ベースのマルウェア (Pushdo、BankPatch、CryptoLocker など) は、多数の疑いのある疑いがある範囲内でアクティブな C2 サーバーの位置を隠すことによってドメインの数がブロックされないように制限し、時刻、暗号化キー、ディクショナリ名の派生スキーム、およびその他の一意の値などの要因に基づいてアルゴリズム的に生成できます。DGA が生成する大抵のドメインは有効なドメインとして解決されませんが、脅威を完全になくすためにはすべてを特定する必要があります。DGA 分析は、DGA で頻繁に使用される他の技術に対してリバース エンジニアリングを行って分析することで、人ではなく機械によってドメインが生成されたと考えられるかどうか判断します。その後 Palo Alto Networks はこれらの特性を使用して未知だった DGA ベースの脅威をリアルタイムで特定し、ブロックします。

- **NXNSAttack** (UTID:109010007）-DNSプロトコルに存在するNXNSAttackの脆弱性は、すべての再帰DNSリゾルバーに影響を及ぼし、悪意のある攻撃者がDDOSのような増幅攻撃を開始して、脆弱な権威DNSサーバーの通常の動作を妨害する可能性があります。NXNSAttack は、再帰 DNS リゾルバーに無効な要求を大量に発行してサーバーをシャットダウンする可能性を強制することで、権限のある DNS サーバーに大量のトラフィックスパイクを発生させる可能性があります。
- **DNS Rebinding** (UTID:109010009) - DNSリバインディング攻撃は、短いTTLパラメータで構成された攻撃者が管理するドメインにユーザーを誘い込み、ドメイン名の解決方法を操作して、ブラウザの同一生成元ポリシーを悪用し迂回させるものです。これにより、悪意のあるアクターは、プライベート ネットワーク内のリソースを攻撃またはアクセスするための仲介役としてクライアント マシンを使用できます。
- **DNS Infiltration** (UTID:109001003) - DNS侵入には、悪意のある行為者が不正なA（IPv4）およびAAAA（IPv6）レコード要求への応答を通じて、微細なペイロードを隠し、解決できるようにするDNSクエリが含まれます。クライアントが複数のサブドメインを解決し、それぞれがエンコードされたコンポーネントを持つA/AAAAレコードを含む場合、それらに含まれるデータを統合して悪意のあるペイロードを形成し、クライアントマシンで実行することが可能です。ペイロードを実行した後、DNSトンネルを確立するためのセカンダリペイロードを導入したり、追加のエクスプロイトを行うことができます。
- **DNS**トラフィック プロファイリング(UTID:109010010)—(Advanced DNSセキュリティが必要) DNSトラフィック プロファイリングは、DNSトラフィック パターンの評価に基づいて、C2接続を確立しようとするマルウェアを検出するクラウドベースのアナライザーです。Advanced DNSセキュリティが組織のDNSトラフィックを監視すると、アウトバウンドDNS要求シーケンスがベクトル化されてDNSトラフィック プロファイルが形成され、一意のDNS要求パターンを特定可能な悪意のあるC2ドメイン プロファイルに関連付けることができるML技術を使用して分析されます。

- ダイナミック**DNS**ホストドメイン （UTID：109020002) —ダイナミックDNS（DDNS）サービスは、ホスト名とIPアドレスのマッピングをほぼリアルタイムで提供し、静的IPが利用できないときに、特定のドメインにリンクしたIPアドレスの変更を維持することができます。これにより、攻撃者は DDNS サービスを使用してネットワークに侵入し、コマンド アンド コントロール サーバーをホストする IP アドレスを変更することができます。マルウェア キャンペーンとエクスプロイト キットは、ペイロード配布戦略の一部として DDNS サービスを利用する可能性があります。ホスト名インフラストラクチャの一部として DDNS ドメインを利用することにより、攻撃者は特定の DNS レコードに関連付けられた IP アドレスを変更し、検出をより簡単に回避できます。DNS セキュリティは、さまざまなソースからの DNS データをフィルタリングおよび相互参照して候補リストを生成し、さらに検証して精度を最大化することにより、悪用される DDNS サービスを検出します。
- **Malware Domains** —悪意のあるドメインは、マルウェアをホストおよび配布し、さまざまな脅威（実行ファイル、スクリプト、ウイルス、ドライブバイダウンロードなど）をインストールしようとするWebサイトを含む可能性があります。悪意のあるドメインは、外部ソースを介して悪意のあるペイロードをネットワークに配信するという点で C2ドメインと区別で

きますが、C2では、感染したエンドポイントは通常、リモート サーバーに接続して、追加の命令やその他の悪意のあるコンテンツを取得しようとします。

- **Malware Compromised DNS** (UTID:109003001）-DNSを侵害するマルウェアには、一見すると本物のように見えるホスト名やサブドメインを生成し、実際には悪意のあるものを生成する、さまざまな手法があります。これには、データベース中心のセキュリティソリューションを偽装したり、誤解させたり、回避したりするために、既存の評判の良いホスト名を模倣した新しく観察されたホスト名が含まれます。これらは、データベースリストへの追加を先取りするために、一括して迅速に生成できます。ドメインシャドウイングは、通常、攻撃者がより一般的な攻撃によってドメインアカウントの制御を取得した後に続きます。これにより、ルートドメインが正当かつ有効であるにもかかわらず、攻撃の調整に使用される不正なサブドメインを作成するために必要なアクセスが提供され、ネットワークセキュリティを回避できる可能性が高くなります。
- ランサムウェア ドメイン (UTID:109003002)—ランサムウェアは、身代金の支払いと引き換えにユーザーがデータにアクセスできないようにロックまたは暗号化するマルウェアのサブカテゴリーです。このマルウェアが実行されると、攻撃者によってシステムがユーザーに解放される可能性があります。ランサムウェアは、悪意のあるランサムウェア ドメインを通じて配布できます。ドメインは、ユーザーが騙されてダウンロードされる一見正当なファイルをホストします。

- **Newly Registered Domains** (UTID:109020001) - 新しく登録されたドメインは、TLD オペレータによって最近追加されたドメイン、または過去 32 日以内に所有権が変更されたドメインです。新しいドメインは正当な目的で作成できますが、大部分は C2サーバーとしての運用やマルウェア、スパム、PUP/アドウェアの配布などの悪意のある行動を促進するために使用されることがよくあります。Palo Alto Networks は、特定のフィード (ドメイン レジストリとレジストラ)を監視し、ゾーンファイル、パッシブ DNS、WHOIS データを使用して登録キャンペーンを検出することにより、登録されたばかりのドメインを検出します。
- **Phishing Domains** (UTID:109010001) —フィッシング ドメインは、フィッシングやファーミングによって正当な Web サイトになりすますことにより、個人情報やユーザーの資格情報などの機密データを送信させるようにユーザーを誘導しようとします。これらの悪意のある活動では、ソーシャルエンジニアリング キャンペーン (一見すると信頼できる送信元がユーザーを操作して、電子メールまたはその他の形式の電子通信を介して個人情報を送信する)、または正当と思われる不正なサイトにユーザーを誘導する Web トラフィック リダイレクトを通じて実行する可能性があります。
- **Grayware Domains** (UTID:109010002) —(PAN-OS コンテンツ リリース 8290 以降のインストールで使用可能)。グレーウェアドメインは、通常、直接的なセキュリティ上の脅威をもたらすものではありませんが、攻撃のベクトルを容易にしたり、さまざまな望ましくない動作を引き起こしたり、単に疑わしい/不快なコンテンツを含む可能性があります。これらには、次のような Web サイトやドメインが含まれます。
  - ユーザーをだましてリモート アクセスを許可するようにします。

- 人気のあるウェブ ホスティングやダイナミック ドメイン ネーム システム（DDNS）サービスのサブドメインを活用して、悪意のあるコンテンツをホストし、配布します（サブドメイン レピュテーション - UTIDL 109002004）。
- アドウェアやその他の未承諾のアプリケーション (暗号マイナー、ハイジャック犯、および PUP (望ましくない可能性のあるプログラム) など) が含まれています。
- 高速フラックス技術によるドメイン識別隠蔽動作の展開 (**fastflux detection** - UTID:109010005).
- DNSセキュリティの予測分析を通じて証明される悪意のある行動と使用法を実証 (悪意のある **NRD** - UTID:109010006).
- 権威あるDNSサーバーのDNSレコードが不適切に設定されているか、または古く、削除またはその他の方法で修正されていないために、正当なソースから悪意のあるウェブサイトへトラフィックをリダイレクトする (ダングリング **DNS** - UTID:109010008).
- 違法行為や詐欺を促進します。
- ブロックリストを回避したり、悪意のあるWebサイトにトラフィックをルーティングすることでワイルドカードDNS攻撃を可能にするために使用できるワイルドカードDNSエントリを含む (ワイルドカードの悪用 - UTID: 109002001).
- 収集したDNSデータから構築された確立されたベースラインプロファイルと比較して、異常な特性を持つDNSトラフィックの存在を示す (異常検出)。
- 数ヶ月または数年前に登録され、休眠状態のままにされ、アクティブになったときに評判チェックをバイパスしている。これには、今まで見られなかった、または評価もされていないといった新たに観察されたドメインも含まれます (戦略的に古いドメイン - UTID:109002002).
- 証明書の透過性ログに基づいて攻撃者が悪意を持って登録した未使用ドメインである（蓄積ドメイン検出-UTID：109002005)。
- 人気ブランドのドメインに酷似し、誤って入力されたウェブ ページのアドレスを使ってユーザーを騙し、その目的は偽造サイトや詐欺サイトにユーザーを誘導することである。(サイバースクワッティング/タイポスクワッティング ドメイン - UTID:109002003)。

- パークドメイン (UTID:109010003)—(PAN-OS コンテンツ リリース 8318 以降のインストールで利用可能) Parked ドメインは、通常、限られたコンテンツをホストする非アクティブな Web サイトであり、多くの場合、ホスト エンティティの収益を生み出す可能性のあるクリックスルー広告の形式で行われますが、一般にエンド ユーザーにとって有用なコンテンツは含まれていません。多くの場合、これらは正当なプレースホルダーとして機能するか、または単なる迷惑行為として機能しますが、マルウェアの配布の可能性のあるベクトルとしても使用される可能性があります。
- プロキシ回避とアノニマイザー（匿名化） (UTID:109010004)—(PAN-OS コンテンツ リリース 8340 以降のインストールで利用可能)Proxy Avoidance and Anonymizers は、コンテンツ フィルタリング ポリシーをバイパスするために使用されるサービスへのトラフィックです。アノニマイザー プロキシ サービスを介して組織のコンテンツ フィルタリング ポリシーを回避しようとするユーザーは、DNS レベルでブロックされます。

- 広告追跡ドメイン(UTID:109004000）—（PAN-OSコンテンツ リリース8586以降のインストールで利用可能）広告追跡ドメインは、ユーザーのエンゲージメント（リンク クリック、ウェブ ページ ナビゲーションなど）を追跡するために、ウェブ ページ用の特定のタイプのマーケティング オートメーション コンテンツを配信します。通常、これらのサードパーティのドメインは、バニティURLを使用して隠蔽され、送信元ドメインの一部であるように表示されます。
  - **CNAME**クローキング(UTID:109004001)—CNAMEクローキングは、サブドメインのWeb要求を同じウェブサイトから送信されたように変更することでURLを隠す代替手段を提供します。ただし、実際には、サブドメインはCNAMEを使用してサードパーティのドメインに解決します。この手法は、疑わしいCNAMEの宛先に接続する可能性のあるブラウザベースのプライバシー保護のいくつかを回避します。
- ハイジャックされたドメイン (UTID:109004000)—(Advanced DNSセキュリティが必要)ハイジャックされたドメインには、正規のドメインを攻撃者が運用するIPアドレスに解決させる能力を攻撃者が得るドメインが含まれます。通常、組織のDNSインフラストラクチャの何らかの側面が侵害されます。これには、DNSプロバイダーへの不正な管理アクセス、DNS解決プロセス中のMiTM攻撃、DNSサーバー自体へのアクセスなどが含まれます。
- ドメインの設定ミス(UTID:109004000）—（Advanced DNSセキュリティが必要）ドメインの設定に誤りがあると、攻撃者はドメイン設定の問題を利用して、組織のDNSに独自の悪意のあるドメインを組み込むことができます。これらの古いDNSレコードは、攻撃者が顧客のサブドメインの所有権を奪い、悪意のある目的でユーザーを攻撃者が管理するIPやウェブサイトにリダイレクトすることを可能にします。これらの解決不能な設定ミスドメインは、高度DNSセキュリティの設定時に指定された公開親ドメインに基づいています。
  - 設定ミス ゾーン:(UTID:109004200）—他の設定ミス カテゴリに対応しない設定ミスドメイン用の汎用カテゴリー。
  - 設定ミス ゾーンダングリング(UTID:109004201)—組織の公開ドメインに存在する権威あるDNSサーバー上のDNSレコードが不適切に設定されているか、古いために、正当な送信元からのトラフィックを悪意のあるウェブサイトにリダイレクトする設定ミスのドメイン。
  - 設定ミス クレーム可能**NX** (UTID:109004202 ）: 組織のDNS構成の一部として定義されているが、すでに存在しない（NXDOMAINS）設定済みのドメインは、攻撃者によって密かに登録され、ユーザーを悪意のあるウェブサイトにリダイレクトするために使用され、攻撃者が顧客のネットワークにアクセスできるようになる可能性があります。

データの収集とロギング

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced DNSセキュリティ ライセンス（拡張機能サポート用）またはDNSセキュリティ ライセンス ❑ Advanced Threat PreventionまたはThreat Preventionライセンス

DNSセキュリティ サービスは、セキュリティ ポリシー ルール、関連するアクション、およびドメイン検索を実行する際のDNSクエリの詳細に基づいて、サーバーの応答と要求情報を収集し、Strata Logging Serviceベースのアクティビティ アプリケーション(AIOps for NGFW Free、Prisma Access、Strata Logging Serviceなど)用にDNSセキュリティのログを生成します。さらに、ネットワーク セキュリティ プラットフォームは補足DNSデータをDNSセキュリティ クラウド サーバーに転送し、Palo Alto Networksサービスによって使用され、より正確なドメイン情報 (プロバイダー ASN、ホスティング情報、位置情報識別など) を提供します。この補足データは DNS セキュリティ サービスを運用するために必要ではありませんが、強化された分析、DNS検出、および予防機能を生成するためのリソースを提供します。このアクションは、データ収集が行われてから30秒以内に実行されます。ファイアウォールのパフォーマンスへの影響を最小限に抑えるため、DNSセキュリティ テレメトリは最小限のオーバーヘッドで動作するため、Strata Logging Serviceに送信される DNSテレメトリ データの総量が制限されます。その結果、DNSクエリのサブセットのみがDNSセキュリティ ログ エントリとしてStrata Logging Serviceに転送されます。そのため、Palo Alto Networksは、悪意のあるDNS要求のログをDNSセキュリティ ログではなく脅威ログとして表示することを推奨しています。

悪意のある*DNS*クエリも脅威ログとして記録され、*PAN-OS*ログ転送を使用して*Strata Logging Service*に送信されます（適切に構成されている場合）。

DNSセキュリティは次のデータ フィールドを送信できます。

項目	の意味
操作	DNS クエリに対して実行されたポリシーアクションを表示します。
タイプ	DNS レコードの種類を表示します。
応答	DNS クエリのドメインが解決した IP アドレス。

項目	の意味
応答コード	DNS クエリに対する応答として受信された DNS 応答コード。
送信元IP	DNS 要求を行ったシステムの IP アドレス。
送信元ユーザー	ファイアウォールの User-ID 機能が有効になっている場合は、DNS リクエスターの ID が表示されます。
Source Zone	セキュリティ ポリシールールで参照されている構成済みのソースゾーン。

DNS の拡張データ収集は、*DNS* 例外の許可リストに追加されたドメインに対してバイパスされます。

潜在的にユーザを識別するために使用できるデータフィールド（送信元 IP、送信元ユーザ、および送信元ゾーン）は、次の CLI コマンドを使用して自動送信から差し控えることができます。**`set deviceconfig`** 設定 **`ctd cloud-dns-privacy-mask`** はい。更新を有効にするには、コミット をコミットする必要があります。

地域サービス ドメイン

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced DNSセキュリティ ライセンス（拡張機能サポート用）またはDNSセキュリティ ライセンス ❑ Advanced Threat PreventionまたはThreat Preventionライセンス

Palo Alto Networksは、DNSセキュリティおよびAdvanced DNSセキュリティの運用にサービスを提供するグローバルおよび地域ドメインのネットワークを管理しています。これらのサービス ドメインは、リアルタイムのDNS要求アナライザーを操作し、DNSシグネチャ データベースにアクセスし、高度なクラウド依存機能を提供します。デフォルトでは、DNSセキュリティとAdvanced DNSセキュリティはグローバル サービス ドメイン(それぞれdns.service.paloaltonetworks.comとadv-dns.service.paloaltonetworks.com)に接続し、ネットワーク セキュリティ プラットフォームの場所に最も近い地域ドメインに自動的にリダイレクトされます。

DNSセキュリティ地域サービス ドメイン

Palo Alto Networksでは、フェイルオーバー処理を改善するために、デフォルトのグローバル サービス ドメイン設定を使用することをお勧めします。ただし、ロケーションの特性が原因で遅延の問題が発生した場合(たとえば、複数の重複する地域ドメインにまたがる場合)は、サービス ドメインを手動で指定できます。DNSセキュリティで使用される地域サービス ドメインを指定するには、DNSサーバー設定の一部として、有効な地域ドメインを示すCNAMEレコードを含む dns.service.paloaltonetworks.comのDNSエントリを追加する必要があります。地域ドメインに接続した後、ファイアウォールでCLIコマンドを発行できます。

```
[show dns-proxy dns-signature counters (dns-proxy dns-signatureカウンターを表示)]
```

をクリックして、平均遅延を確認します。関連セクションは、シグネチャ クエリAPIの見出しの下にあります。

次の表に、DNSセキュリティ サービスのドメインを示します。

場所	URL
ケープタウン、南アフリカ	dns-za.service.paloaltonetworks.com
香港	dns-hk.service.paloaltonetworks.com
東京、日本	dns-jp.service.paloaltonetworks.com
シンガポール	dns-sg.service.paloaltonetworks.com
ムンバイ、インド	dns-in.service.paloaltonetworks.com
シドニー、オーストラリア	dns-au.service.paloaltonetworks.com
ロンドン、英国	dns-uk.service.paloaltonetworks.com
フランクフルト、ドイツ	dns-de.service.paloaltonetworks.com
エームスハーヴェン、オランダ	dns-nl.service.paloaltonetworks.com
パリ、フランス	dns-fr.service.paloaltonetworks.com
バーレーン	dns-bh.service.paloaltonetworks.com
モントリオール、ケベック、カナダ	dns-ca.service.paloaltonetworks.com
オザスコ、サンパウロ、ブラジル	dns-br.service.paloaltonetworks.com
カウンシルブラフス、アイオワ、米国	dns-us-ia.service.paloaltonetworks.com
アッシュバーン、北バージニア、米国	dns-us-va.service.paloaltonetworks.com
ザ・ダレス、オレゴン、米国	dns-us-or.service.paloaltonetworks.com
ロサンゼルス、カリフォルニア、米国	dns-us-ca.service.paloaltonetworks.com

Advanced DNSセキュリティ地域サービス ドメイン

Advanced DNSセキュリティ クエリを容易にするために使用するサーバーを手動で指定できます。Palo Alto Networksではデフォルトのグローバル サービス ドメインの使用を推奨しています

が、予想よりも高い遅延やその他のサービス関連の問題が発生した場合は、選択したサーバーをオーバーライドできます。

PAN-OSのAdvanced DNS Securityサービス ドメインは、**[Device (デバイス)]** > **[Setup (セットアップ)]** > **[Management (管理)]** > **[Advanced DNS Security (Advanced DNSセキュリティ)]** > **[DNS Security Server （DNSセキュリティ サーバー]**で指定できます。

この設定は、標準の*DNS*セキュリティ クエリの処理方法には影響しません。

次の表に、Advanced DNSセキュリティ サービス ドメインを示します。

場所	URL
ケープタウン、南アフリカ	za.adv-dns.service.paloaltonetworks.com
バーレーン	bh.adv-dns.service.paloaltonetworks.com
香港	hk.adv-dns.service.paloaltonetworks.com
東京、日本	jp.adv-dns.service.paloaltonetworks.com
シンガポール	sg.adv-dns.service.paloaltonetworks.com
ムンバイ、インド	in.adv.dns.service.paloaltonetworks.com
シドニー、オーストラリア	au.adv-dns.service.paloaltonetworks.com
ロンドン、英国	uk.adv-dns.service.paloaltonetworks.com
フランクフルト、ドイツ	de.adv.dns.service.paloaltonetworks.com
エームスハーヴェン、オランダ	nl.adv.dns.service.paloaltonetworks.com
パリ、フランス	fr.adv-dns.service.paloaltonetworks.com
バーレーン	bh.adv-dns.service.paloaltonetworks.com
モントリオール、ケベック、カナダ	ca.adv.dns.service.paloaltonetworks.com
オザスコ、サンパウロ、ブラジル	br.adv.dns.service.paloaltonetworks.com
カウンシルブラフス、アイオワ、米国	us-ia.adv.dns.service.paloaltonetworks.com

場所	URL
アッシュバーン、北バージニア、米国	us-va.adv.dns.service.paloaltonetworks.com
ザ・ダレス、オレゴン、米国	us-or.adv.dns.service.paloaltonetworks.com
ロサンゼルス、カリフォルニア、米国	us-ca.adv.dns.service.paloaltonetworks.com

DNSセキュリティ サブスクリプション サービスの設定

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced DNS Securityライセンス（拡張機能サポート用）またはDNS Securityライセンス ❑ Advanced Threat PreventionまたはThreat Preventionライセンス

Advanced DNS SecurityまたはDNSセキュリティを有効化および設定する前に、運用元のプラットフォーム ライセンスに加えて、Threat Prevention（またはAdvanced Threat Prevention）ライセンスおよびAdvanced DNS SecurityまたはDNS Securityライセンスを取得およびインストールする必要があります。ライセンスはPalo Alto Networksカスタマー サポート ポータルからアクティベートされ、DNS分析を行う前にアクティベートされている必要があります。さらに、DNSセキュリティ サブスクリプション サービス（他のPalo Alto Networksのセキュリティ サービスと同様）は、セキュリティ プロファイルを通じて管理されます。セキュリティ プロファイルは、セキュリティ ポリシー ルールを通じて定義されたネットワーク適用ポリシーの設定に依存します。DNSセキュリティ サブスクリプション サービスを有効にする前に、セキュリティ サブスクリプションが有効になっているセキュリティ プラットフォームのコア コンポーネントについて理解しておくことをお勧めします。詳細については、製品マニュアルを参照してください。

DNSセキュリティ サブスクリプション サービスを有効にして、ネットワーク セキュリティのデプロイメントで最適に機能するように設定するには、以下の作業を参照してください。ここに示すすべてのプロセスを実装する必要はありませんが、デプロイメントを成功させるために、すべてのタスクを見直して利用可能なオプションに慣れることをお勧めします。最適な操作性とセキュリティを実現するためには、Palo Alto Networksが提供するベストプラクティスに従うことがさらに推奨されます。

- DNS脅威がネットワークに侵入するのを防ぐために、ネットワーク セキュリティ プラットフォームでDNSセキュリティまたは高度なDNSセキュリティを有効にする(必須)
- ドメイン シグネチャの例外を作成し、リストが誤検知を制限し、内部DNSサーバーがDNS分類をトリガーしないようにする
- 使用可能なドメイン カテゴリーに対して設定されたポリシー アクションをテストする
- DNS セキュリティ サービスへのファイアウォールの接続を確認する

- ファイアウォールのDNSルックアップ タイムアウト設定をカスタマイズして、自分の遅延による接続のドロップを制限する

DNS セキュリティの有効化

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced DNSセキュリティ ライセンス（拡張機能サポート用）またはDNSセキュリティ ライセンス ❑ Advanced Threat PreventionまたはThreat Preventionライセンス

DNSセキュリティを有効にするには、DNSセキュリティ サービスにアクセスするためのアンチスパイウェア セキュリティ プロファイルを作成 (または変更) し、DNSシグネチャ カテゴリー(複数可) のログ重大度とポリシー設定を構成し、プロファイルをセキュリティ ポリシー ルールにアタッチする必要があります。

- Strata Cloud Manager
- PAN-OS & Panorama

DNSセキュリティの有効化 (Strata Cloud Manager)

STEP 1 | Palo Alto Networksのサポート アカウントに関連付けられた資格情報を使用し、ハブ上のStrata Cloud Managerにログインします。

STEP 2 | DNSセキュリティとThreat Prevention (またはAdvanced Threat Prevention)のライセンスがアクティブであることを確認します。**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFW]Prisma Access** > **[Overview (概要)]**を選択し、**[License (ライセンス)]**パネルのライセンス使用条件のリンクをクリックします。次のセキュリティ サービスの横に緑色のチェック マークが表示されます。アンチウイルス、アンチスパイウェア、脆弱性防御、DNSセキュリティ。

STEP 3 | セキュリティ ポリシーの *paloalto-dns-security* App-ID が、DNS セキュリティ クラウド セキュリティ サービスからの のトラフィックを有効にする に構成されていることを確認します。

> *App-ID* セキュリティ ポリシーを適用するように構成されたインターネットに接続する境界ファイアウォールを使用して、ファイアウォールの展開によって管理トラフィックがルーティングされる場合は、境界ファイアウォールで *App-ID* を許可する必要があります。これを行わないと、*DNS* セキュリティ接続ができなくなります。

STEP 4 | 定義されたシンクホールに悪意のあるDNSクエリを送信するように、DNSセキュリティ シグネチャ ポリシー設定を構成します。

ドメイン許可リストとして外部動的リストを使用する場合、*DNS* セキュリティ ドメイン ポリシーの動作よりも優先されません。その結果、*EDL* のエントリと *DNS* セキュリティ ドメイン カテゴリに一致するドメインがある場合、*EDL* が許可のアクションで明示的に構成されている場合でも、*DNS* セキュリティで指定されたアクションは適用されます。*DNS*ドメインの例外を追加する場合は、アラート アクションを使用して*EDL*を構成するか、 *[DNS Exceptions (DNS*例外*)]*タブにある*[DNS Domain/FQDN Allow List (DNS* ドメイン*/FQDN* 許可リスト*)]*に追加します。

1. **[Manage (**管理**)]** > **[Configuration (**設定**)]** > **[NGFW]Prisma Access** > **[Security Services (**セキュリティ サービス**)]** > **[DNS Security (DNS**セキュリティ**)]**を選択します。
2. 既存のDNSセキュリティ プロファイルを作成または変更します。
3. プロファイルに **Name (**名前**)** を付け、任意で説明を入力します。
4. **[DNS Categories (DNS**カテゴリー**)]**セクションのDNSセキュリティ見出しの下に、個別に設定可能な DNS シグネチャ送信元があり、個別のポリシー アクションとパケット キャプチャ設定を定義できます。

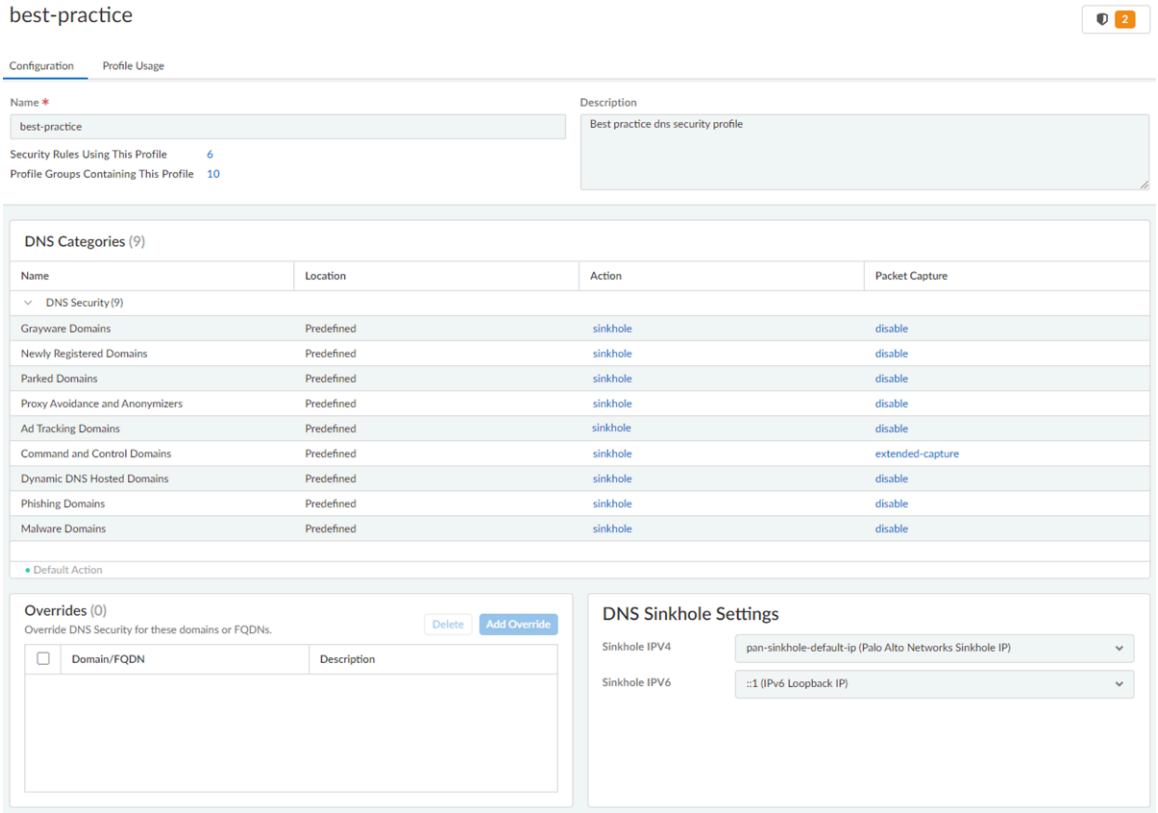
   *Palo Alto Networks*では、全てのシグネチャ送信元のデフォルトのアクション設定を使用して、最適なカバレッジを確保し、インシデントの応答と修復を支援することを推奨しています。*DNS*セキュリティ設定を設定するためのベストプラクティスに関する詳細は、ネットワークをレイヤー4およびレイヤー7の回避から保護するためのベストプラクティスを参照してください。

   - DNS セキュリティ シグネチャ ソースの既知のマルウェア サイトに対して DNS ルックアップが行われる際に行うアクションを選択します。ここでは alert (アラート)、allow (許可)、block (ブロック)、sinkhole (シンクホール) を使用できます。Palo Alto Networksは、アクションをシンクホールに設定することを推奨しています。
   - DNS トラフィック検査を完全にバイパスするには、ポリシー アクションを **Allow** に設定し、対応するログ重大度を **None** に構成します。
   - （任意）**Packet Capture (**パケット キャプチャ **- pcap)** ドロップダウンリストにて、セッションの最初のパケットをキャプチャする場合は**single-packet**を、1～50の間で設定を行うには**extended-capture**を選択します。その後、packet capture (パケット キャプチャ - pcap) を使用してさらに解析できます。
5. **[DNS Sinkhole Settings (DNS**シンクホール設定**)]**セクションで、有効なシンクホール アドレスが存在することを確認します。便宜上、デフォルト設定（pan-sinkhole-default-ip）はPalo Alto Networksのシンクホール サーバーにアクセスするように設定されてい

ます。Palo Alto Networksは、更新によりこのアドレスを自動的に更新する場合があります。

シンクホールは、指定されたシンクホール サーバーに対するシンクホール アクションに設定された*DNS*カテゴリーに一致するドメインに対する*DNS*クエリへの応答を偽造し、侵害されたホストの特定を支援します。デフォルトのシンクホール *FQDN* が使用される場合、*firewall* は、内部 *DNS* サーバーが *CNAME* レコードを解決することを期待して、*CNAME* レコードを応答としてクライアントに送信し、クライアントから構成済みのシンクホール・サーバーへの悪意のある通信をログに記録し、容易に識別できるようにします。ただし、内部*DNS*サーバーのないネットワークにいる場合、または*CNAME*を*A*レコード応答に適切に解決できない他のソフトウェアやツールを使用している場合、*DNS*要求はドロップされ、脅威解析に不可欠な不完全なトラフィック ログの詳細が生成されます。これらのインスタンスでは、次のシンクホール*IP*アドレスを使用する必要があります。*(72.5.65.111)*。

Sinkhole IPv4 (シンクホール **IPv4)** あるいは**Sinkhole IPv6 (**シンクホール **IPv6)** アドレスをネットワーク上のローカル サーバーあるいはループバック アドレスに変更する場合はネットワーク上のローカル サーバーにシンクホールIPアドレスを設定をご覧ください。



6. **[OK]** をクリックしてDNSセキュリティ プロファイルを保存します。

STEP 5 | DNSセキュリティ プロファイルをセキュリティ ポリシー ルールにアタッチします。

STEP 6 | ポリシー アクションが適用されているかどうかテストします。

1. DNS Securityのテスト ドメインにアクセスして、特定の脅威タイプのポリシー アクションが実施されていることを確認します。
2. アクティビティを監視するには
   1. アクティビティ ログを表示し、シンクホールしたアクションでURLドメインを検索し、アクセスしたテスト ドメインのログ エントリを表示します。

STEP 7 | オプション: DNS-over-TLS/ポート853トラフィックを復号化する復号化ポリシー ルールを作成します。復号化されたDNSペイロードは、DNSポリシー設定を含むDNSセキュリティ プロファイル設定を使用して処理できます。TLSトラフィックを介したDNSセキュリティが復号化されると、脅威ログに記録されるDNS要求は送信元ポートが853の従来の**dns**ベースのアプリケーションとして表示されます。

STEP 8 | その他のモニタリング オプションについては、DNSセキュリティ サブスクリプション サービスの監視を参照してください

DNSセキュリティの有効化 (NGFW (Managed by PAN-OS or Panorama))

PAN-OS 10.0以降では、個別に設定可能なDNSシグネチャ ソースがサポートされており、特定のシグニチャ ソースに対してログの重大度レベルだけでなく、個別のポリシー アクションを定義することができます。これにより、ネットワーク セキュリティ プロトコルに従って、ドメイン タイプの脅威ポスチャに基づいて、個別の正確なセキュリティ アクションを作成できます。DNSシグネチャの送信元定義はPAN-OSコンテンツ リリースを通じて拡張可能であるため、新しいDNSセキュリティ アナライザーが導入された場合、脅威の性質に基づいて特定のポリシーを作成できます。PAN-OS 10.0以降にアップグレードすると、DNS セキュリティ ソースが新しいカテゴリに再定義され、拡張されたきめ細かな制御が得られます。その結果、新しいカテゴリは以前に定義されたアクションを上書きし、デフォルト設定を取得します。新しく定義された DNS セキュリティ カテゴリに適したシンクホール、ログの重大度、およびパケット キャプチャの設定を必ず再適用してください。

- PAN-OS 11.0以降
- PAN-OS 10.x
- PAN-OS 9.1

DNSセキュリティの有効化（PAN-OS 11.0以降）

STEP 1 | NGFWにログインします。

STEP 2 | DNSセキュリティを利用するには、DNSセキュリティとThreat Prevention（またはAdvanced Threat Prevention）の有効なサブスクリプションが必要です。

必要なサブスクリプションがあることを確認します。現在ライセンスを持っているサブスクリプションを確認するには、**Device**（デバイス）> **Licenses(**ライセンス**)** を選択し、適切なライセンスが表示され、有効期限が切れていないことを確認します。

STEP 3 | セキュリティ ポリシーの *paloalto-dns-security* App-ID が、DNS セキュリティ クラウド セキュリティ サービスからの のトラフィックを有効にする に構成されていることを確認します。

App-ID セキュリティ ポリシーを適用するように構成されたインターネットに接続する境界ファイアウォールを使用して、ファイアウォールの展開によって管理トラフィックがルーティングされる場合は、境界ファイアウォールで *App-ID* を許可する必要があります。これを行わないと、*DNS* セキュリティ接続ができなくなります。

STEP 4 | 定義されたシンクホールに悪意のあるDNS クエリを送信するように、DNSセキュリティ シグネチャ ポリシー設定を構成します。

ドメイン許可リストとして外部動的リストを使用する場合、*DNS* セキュリティ ドメイン ポリシーの動作よりも優先されません。その結果、*EDL* のエントリと *DNS* セキュリティ ドメイン カテゴリに一致するドメインがある場合、*EDL* が許可のアクションで明示的に構成されている場合でも、*DNS* セキュリティで指定されたアクションは適用されます。*DNS*ドメインの例外を追加する場合は、アラート アクションを使用して*EDL*を構成するか、 *[DNS Exceptions (DNS*例外*)]*タブにある*[DNS Domain/FQDN Allow List (DNS* ドメイン*/FQDN* 許可リスト*)]*に追加します。

1. **Objects (**オブジェクト**) > > Security Profiles (**セキュリティ プロファイル**) > > Anti-Spyware (**アンチスパイウェア**)** を選択します。
2. 既存のプロファイルを変更あるいはプロファイルを作成するか、既存のデフォルト プロファイルの 1 つを選択してコピーします。
3. プロファイルに **Name (**名前**)** を付け、任意で説明を入力します。
4. **DNS Policies (DNS** ポリシー**)** タブを選択します。
5. **Signature Source (**シグネチャ送信元**)**列にある DNS セキュリティ見出しの下に、個別に設定可能な DNS シグネチャ送信元があり、個別のポリシー アクションとログの重大度レベルを定義できます。

   Palo Alto Networks では、シグネチャ送信元のデフォルトの *DNS* ポリシー設定を変更して、最適なカバレッジを確保し、インシデントの応答と修復を支援することを推奨しています。ネットワークをレイヤー4およびレイヤー7 回避から保護するためのベストプラクティスで概説されているように、*DNS*セキュリティ設定を設定するためのベストプラクティスに従ってください。

   - ファイアウォールが DNS シグネチャに一致するドメインを検出したときに記録される、ログの重大度レベルを指定します。様々なログ重大度レベルの詳細情報は、Threat Severity Levels (脅威の重大度レベル) を参照してください。
   - DNS セキュリティ シグネチャ ソースの既知のマルウェア サイトに対して DNS ルックアップが行われる際に行うアクションを選択します。オプションはdefault (デフォルト)、allow (許可)、block (ブロック)、またはsinkhole (シンクホール)です。アクションがシンクホールに設定されていることを検証します。
   - DNS トラフィック検査を完全にバイパスするには、ポリシー アクションを **Allow** に設定し、対応するログ重大度を **None** に構成します。
   - （任意）**Packet Capture (**パケット キャプチャ **- pcap)** ドロップダウンリストにて、セッションの最初のパケットをキャプチャする場合は**single-packet**を、1～50の間

で設定を行うには**extended-capture**を選択します。その後、packet capture (パケットキャプチャ - pcap) を使用してさらに解析できます。

6. **DNS Sinkhole Settings (DNS** シンクホール設定**)** セクションで **Sinkhole (**シンクホール**)** が有効になっていることを確認します。便宜を図るため、デフォルトのシンクホールのアドレス (sinkhole.paloaltonetworks.com) は Palo Alto Networks サーバーにアクセスするよう設定されています。Palo Alto Networks はコンテンツ更新によりこのアドレスを自動的に更新する場合があります。

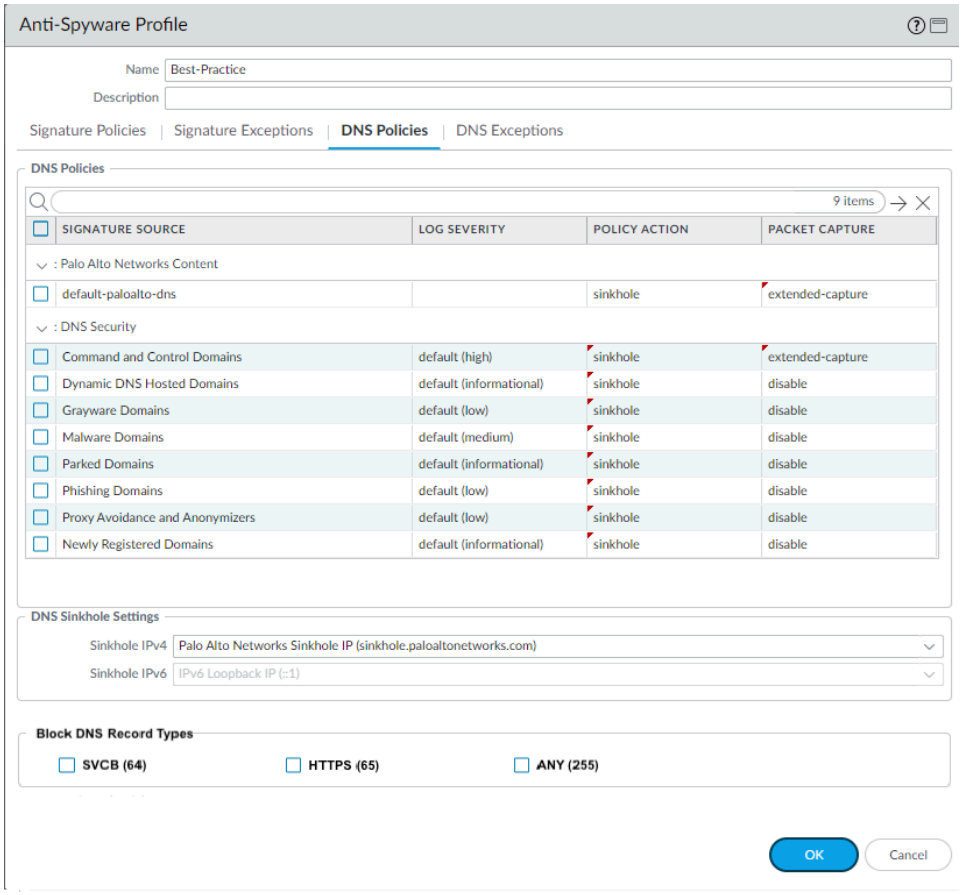
   シンクホールは、指定されたシンクホール サーバーに対するシンクホール アクションに設定された*DNS*カテゴリーに一致するドメインに対する*DNS*クエリへの応答を偽造し、侵害されたホストの特定を支援します。デフォルトのシンクホール*FQDN (sinkhole.paloaltonetworks.com)*が使用される場合、ファイアウォールは、内部*DNS*サーバーが*CNAME*レコードを解決することを期待して、*CNAME*レコードを応答としてクライアントに送信し、クライアントから構成済みのシンクホール・サーバーへの悪意のある通信をログに記録し、容易に識別できるようにします。ただし、内部*DNS*サーバーのないネットワークにいる場合、または*CNAME*を*A*レコード応答に適切に解決できない他のソフトウェアやツールを使用している場合、*DNS* 要求はドロップされ、脅威解析に不可欠な不完全なトラフィック ログの詳細が生成されます。これらのインスタンスでは、次のシンクホール*IP*アドレスを使用する必要があります。*(72.5.65.111)*。

   Sinkhole IPv4 (シンクホール **IPv4)** あるいは**Sinkhole IPv6 (**シンクホール **IPv6)** アドレスをネットワーク上のローカル サーバーあるいはループバック アドレスに変更する場合

はネットワーク上のローカル サーバーにシンクホールIPアドレスを設定をご覧ください。

7. （オプション）後続のTLS接続でClient Helloの暗号化中にキー情報の交換に使用される、指定されたDNSリソース レコード タイプのレコード タイプをブロックします。次のDNS RRタイプを使用できます。SVCB（64）、HTTPS（65）、ANY（255）。

   - *DoH*上の*DNS*セキュリティを有効にするために*ECH*をブロックする必要はありませんが、*Palo Alto Networks*では現在、最適なセキュリティを実現するために、*ECH*が使用するすべての*DNS*レコー ドタイプをブロックすることを推奨しています。
   - タイプ*64*およびタイプ*65*のリソース レコード規格は、まだ流動的（ドラフト状態）であり、変更される可能性があります。*DNS SVCB RR*および*HTTPS RR*の詳細については、次を参照してください。IETFの定義に従って*DNS*（*DNS SVCB*および*HTTPS RR*）を介したサービス バインディングとパラメータ指定。



8. **OK** をクリックし、アンチスパイウェア プロファイルを保存します。

STEP 5 | アンチスパイウェア プロファイルをセキュリティポリシールールに適用します。

1. **Policies**（ポリシー）> **Security**（セキュリティ）の順に選択します。
2. **Security Policy Rule (**セキュリティポリシー ルール**)** を選択するか、作成します。
3. **Actions (**アクション**)**タブで、**Log at Session End (**セッション終了時にログを記録**)**チェック ボックスをオンにして、ログを有効にします。
4. Profile Setting [プロファイル設定]セクションで**Profile Type**[プロファイルタイプ]ドロップダウンリストをクリックし、すべての**Profiles**[プロファイル]を表示します。**Anti-Spyware (**アンチスパイウェア**)** ドロップダウンリストで、新しい、あるいは修正したプロファイルを選択します。
5. **[OK]** をクリックしてポリシー ルールを保存します。

STEP 6 | ポリシー アクションが適用されているかどうかテストします。

1. DNSセキュリティのテスト ドメインにアクセスして、特定の脅威タイプのポリシー アクションが実施されていることを確認します。
2. ファイアウォール上のアクティビティを監視するには：
   1. **ACC**を選択し、URL Domain [URLドメイン]をグローバルフィルターとして追加し、アクセスしたドメインのThreat Activity [脅威アクティビティ]およびBlocked Activity [ブロックされたアクティビティ]を確認します。
   2. **Monitor (**監視**)** > **Logs (**ログ**)** > **Threat (**脅威**)** を選択し、`(action eq sinkhole)` でフィルタリングしてシンクホールされたドメインのログを確認します。
   3. その他のモニタリング オプションについては、DNSセキュリティ サブスクリプション サービスの監視を参照してください。

STEP 7 | オプション: DNS-over-TLS/ポート853トラフィックを復号化する復号ポリシー ルールを作成します。復号化されたDNSペイロードは、DNSポリシー設定を含むアンチスパイウェア プロファイル設定を使用して処理できます。TLSトラフィックを介したDNSセキュリティが復号化されると、脅威ログに記録されるDNS要求は送信元ポートが853の従来のdnsベースのアプリケーションとして表示されます。

STEP 8 | オプション: 悪意のあるドメインへの接続を試みた感染ホストを確認

DNSセキュリティの有効化（PAN-OS 10.x）

STEP 1 | NGFWにログインします。

STEP 2 | DNSセキュリティを利用するには、DNSセキュリティとThreat Prevention（またはAdvanced Threat Prevention）の有効なサブスクリプションが必要です。

必要なサブスクリプションがあることを確認します。現在ライセンスを持っているサブスクリプションを確認するには、**Device**（デバイス）> **Licenses(**ライセンス**)** を選択し、適切なライセンスが表示され、有効期限が切れていないことを確認します。

STEP 3 | セキュリティ ポリシーの *paloalto-dns-security* App-ID が、DNS セキュリティ クラウド セキュリティ サービスからの のトラフィックを有効にする に構成されていることを確認します。

App-ID セキュリティ ポリシーを適用するように構成されたインターネットに接続する境界ファイアウォールを使用して、ファイアウォールの展開によって管理トラフィックがルーティングされる場合は、境界ファイアウォールで *App-ID* を許可する必要があります。これを行わないと、*DNS* セキュリティ接続ができなくなります。

STEP 4 | 定義されたシンクホールに悪意のあるDNSクエリを送信するように、DNSセキュリティ シグネチャ ポリシー設定を構成します。

ドメイン許可リストとして外部動的リストを使用する場合、*DNS* セキュリティ ドメイン ポリシーの動作よりも優先されません。その結果、*EDL* のエントリと *DNS* セキュリティ ドメイン カテゴリに一致するドメインがある場合、*EDL* が許可のアクションで明示的に構成されている場合でも、*DNS* セキュリティで指定されたアクションは適用されます。*DNS* ドメインの例外を追加する場合は、アラート アクションを使用して*EDL*を設定するか、 *[DNS Exceptions (DNS*例外*)]*タブにある*[DNS Domain/FQDN Allow List (DNS* ドメイン*/FQDN* 許可リスト*)]*に追加します。

1. **Objects (**オブジェクト**) > > Security Profiles (**セキュリティ プロファイル**) > > Anti-Spyware (**アンチスパイウェア**)** を選択します。
2. 既存のプロファイルを変更あるいはプロファイルを作成するか、既存のデフォルト プロファイルの 1 つを選択してコピーします。
3. プロファイルに **Name (**名前**)** を付け、任意で説明を入力します。
4. **DNS Policies (DNS** ポリシー**)** タブを選択します。
5. **Signature Source (**シグネチャ送信元**)**列にある DNS セキュリティ見出しの下に、個別に設定可能な DNS シグネチャ送信元があり、個別のポリシー アクションとログの重大度レベルを定義できます。

   Palo Alto Networks では、シグネチャ送信元のデフォルトの *DNS* ポリシー設定を変更して、最適なカバレッジを確保し、インシデントの応答と修復を支援することを推奨しています。ネットワークをレイヤー4 およびレイヤー7 回避から保護するためのベストプラクティスで概説されているように、*DNS*セキュリティ設定を設定するためのベストプラクティスに従ってください。

   - ファイアウォールが DNS シグネチャに一致するドメインを検出したときに記録される、ログの重大度レベルを指定します。様々なログ重大度レベルの詳細情報は、Threat Severity Levels (脅威の重大度レベル) を参照してください。
   - DNS セキュリティ シグネチャ ソースの既知のマルウェア サイトに対して DNS ルックアップが行われる際に行うアクションを選択します。オプションはdefault (デフォルト)、allow (許可)、block (ブロック)、またはsinkhole (シンクホール)です。アクションがシンクホールに設定されていることを検証します。
   - DNS トラフィック検査を完全にバイパスするには、ポリシー アクションを **Allow** に設定し、対応するログ重大度を **None** に構成します。
   - （任意）**Packet Capture (**パケット キャプチャ **- pcap)** ドロップダウンリストにて、セッションの最初のパケットをキャプチャする場合は**single-packet**を、1～50の間

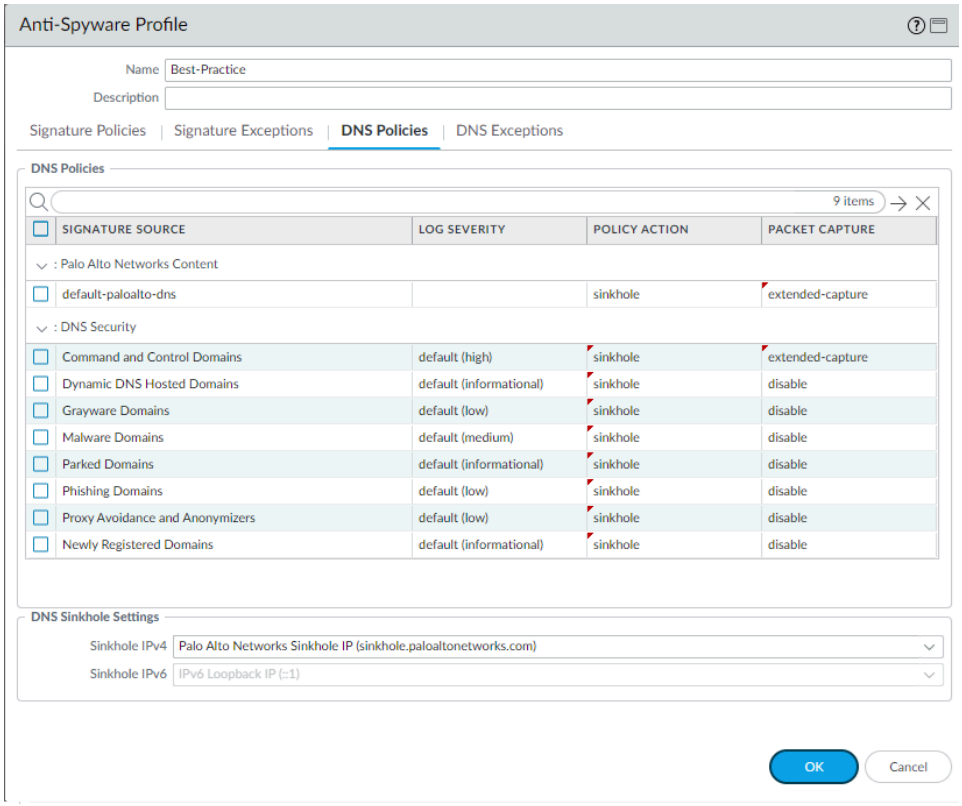
で設定を行うには**extended-capture**を選択します。その後、packet capture (パケットキャプチャ - pcap) を使用してさらに解析できます。

6. **DNS Sinkhole Settings (DNS** シンクホール設定**)** セクションで **Sinkhole (**シンクホール**)** が有効になっていることを確認します。便宜を図るため、デフォルトのシンクホールのアドレス (sinkhole.paloaltonetworks.com) は Palo Alto Networks サーバーにアクセスするよう設定されています。Palo Alto Networks はコンテンツ更新によりこのアドレスを自動的に更新する場合があります。

   シンクホールは、指定されたシンクホール サーバーに対するシンクホール アクションに設定された*DNS*カテゴリーに一致するドメインに対する*DNS*クエリへの応答を偽造し、侵害されたホストの特定を支援します。デフォルトのシンクホール*FQDN (sinkhole.paloaltonetworks.com)*が使用される場合、ファイアウォールは、内部*DNS*サーバーが*CNAME*レコードを解決することを期待して、*CNAME*レコードを応答としてクライアントに送信し、クライアントから構成済みのシンクホール・サーバーへの悪意のある通信をログに記録し、容易に識別できるようにします。ただし、内部*DNS*サーバーのないネットワークにいる場合、または*CNAME*を*A*レコード応答に適切に解決できない他のソフトウェアやツールを使用している場合、*DNS*要求はドロップされ、脅威解析に不可欠な不完全なトラフィック ログの詳細が生成されます。これらのインスタンスでは、次のシンクホール*IP*アドレスを使用する必要があります。*(72.5.65.111)*。

   Sinkhole IPv4 (シンクホール **IPv4)** あるいは**Sinkhole IPv6 (**シンクホール **IPv6)** アドレスをネットワーク上のローカル サーバーあるいはループバック アドレスに変更する場合

はネットワーク上のローカル サーバーにシンクホールIPアドレスを設定をご覧ください。



7. **OK** をクリックし、アンチスパイウェア プロファイルを保存します。

STEP 5 | アンチスパイウェア プロファイルをセキュリティポリシールールに適用します。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。
2. **Security Policy Rule (**セキュリティポリシー ルール**)** を選択するか、作成します。
3. **Actions (**アクション**)**タブで、**Log at Session End (**セッション終了時にログを記録**)**チェック ボックスをオンにして、ログを有効にします。
4. Profile Setting [プロファイル設定]セクションで**Profile Type**[プロファイルタイプ]ドロップダウンリストをクリックし、すべての**Profiles**[プロファイル]を表示します。**Anti-Spyware (**アンチスパイウェア**)** ドロップダウンリストで、新しい、あるいは修正したプロファイルを選択します。
5. **[OK]** をクリックしてポリシー ルールを保存します。

STEP 6 | ポリシー アクションが適用されているかどうかテストします。

1. DNS Securityのテスト ドメインにアクセスして、特定の脅威タイプのポリシー アクションが実施されていることを確認します。
2. ファイアウォール上のアクティビティを監視するには：
   1. **ACC**を選択し、URL Domain [URLドメイン]をグローバルフィルターとして追加し、アクセスしたドメインのThreat Activity [脅威アクティビティ]およびBlocked Activity [ブロックされたアクティビティ]を確認します。
   2. **Monitor (**監視**)** > **Logs (**ログ**)** > **Threat (**脅威**)** を選択し、`(action eq sinkhole)` でフィルタリングしてシンクホールされたドメインのログを確認します。
   3. その他のモニタリング オプションについては、DNSセキュリティ サブスクリプション サービスの監視を参照してください。

STEP 7 | オプション: DNS-over-TLS/ポート853トラフィックを復号化する復号ポリシー ルールを作成します。復号化されたDNSペイロードは、DNSポリシー設定を含むアンチスパイウェア プロファイル設定を使用して処理できます。TLSトラフィックを介したDNSセキュリティが復号化されると、脅威ログに記録されるDNS要求は送信元ポートが853の従来のdnsベースのアプリケーションとして表示されます。

STEP 8 | オプション: 悪意のあるドメインへの接続を試みた感染ホストを確認

DNSセキュリティの有効化（PAN-OS 9.1）

STEP 1 | NGFWにログインします。

STEP 2 | DNSセキュリティを利用するには、DNSセキュリティと有効な脅威防御サブスクリプションが必要です。

必要なサブスクリプションがあることを確認します。現在ライセンスを持っているサブスクリプションを確認するには、**Device**（デバイス） > **Licenses(**ライセンス**)** を選択し、適切なライセンスが表示され、有効期限が切れていないことを確認します。

STEP 3 | セキュリティ ポリシーの *paloalto-dns-security* App-ID が、DNS セキュリティ クラウド セキュリティ サービスからの のトラフィックを有効にする に構成されていることを確認します。

App-ID セキュリティ ポリシーを適用するように構成されたインターネットに接続する境界ファイアウォールを使用して、ファイアウォールの展開によって管理トラフィックがルーティングされる場合は、境界ファイアウォールで *App-ID* を許可する必要があります。これを行わないと、*DNS* セキュリティ接続ができなくなります。

STEP 4 | 定義されたシンクホールにマルウェア DNS クエリを送信するように、DNS セキュリティ署名ポリシー設定を構成します。

ドメイン許可リストとして外部動的リストを使用する場合、*DNS* セキュリティ ドメイン ポリシーの動作よりも優先されません。その結果、*EDL* のエントリと *DNS* セキュリティ ドメイン カテゴリに一致するドメインがある場合、*EDL* が許可のアクションで明示的に構成されている場合でも、*DNS* セキュリティで指定されたアクションは適用されます。*DNS*ドメインの例外を追加したい場合は、アラート アクションで*EDL*を設定することができます。

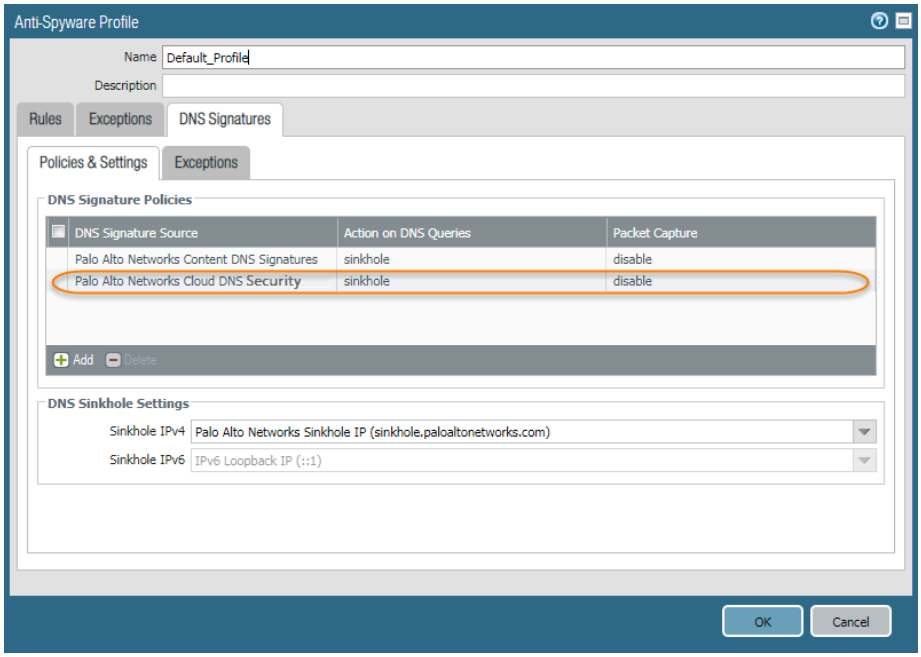
1. **Objects (**オブジェクト**) > > Security Profiles (**セキュリティ プロファイル**) > > Anti-Spyware (**アンチスパイウェア**)** を選択します。
2. 既存のプロファイルを変更あるいはプロファイルを作成するか、既存のデフォルト プロファイルの 1 つを選択してコピーします。
3. プロファイルに **Name (**名前**)** を付け、任意で説明を入力します。
4. **DNS Signatures (DNS** シグネチャ**) > Policies & Settings (**ポリシーおよび設定**)** タブを選択します。
5. **Palo Alto Networks DNS Security (DNS** セキュリティ**)** ソースが表示されない場合は、**Add (**追加**)** をクリックしてリストから選択します。
6. DNS セキュリティ シグネチャ ソースの既知のマルウェア サイトに対して DNS ルックアップが行われる際に行うアクションを選択します。ここでは alert (アラート)、allow (許可)、block (ブロック)、sinkhole (シンクホール) を使用できます。アクションがシンクホールに設定されていることを検証します。
7. （任意）**Packet Capture (**パケット キャプチャ**)** ドロップダウンリストにて、セッションの最初のパケットをキャプチャする場合は**single-packet**を、1～50の間で設定を行うには**extended-capture**を選択します。その後、パケット キャプチャを使用してさらに分析できます。
8. **DNS Sinkhole Settings (DNS** シンクホール設定**)** セクションで **Sinkhole (**シンクホール**)** が有効になっていることを確認します。便宜を図るため、デフォルトのシンクホールのアドレス (sinkhole.paloaltonetworks.com) は Palo Alto Networks サーバーにアクセスする

よう設定されています。Palo Alto Networks はコンテンツ更新によりこのアドレスを自動的に更新する場合があります。

シンクホールは、指定されたシンクホール サーバーに対するシンクホール アクションに設定された*DNS*カテゴリーに一致するドメインに対する*DNS*クエリへの応答を偽造し、侵害されたホストの特定を支援します。デフォルトのシンクホール*FQDN (sinkhole.paloaltonetworks.com)* が使用される場合、ファイアウォールは、内部*DNS*サーバーが*CNAME*レコードを解決することを期待して、*CNAME*レコードを応答としてクライアントに送信し、クライアントから設定済みのシンクホール サーバーへの悪意のある通信をログに記録し、容易に識別できるようにします。ただし、内部*DNS*サーバーのないネットワークにいる場合、または*CNAME*を*A*レコード応答に適切に解決できない他のソフトウェアやツールを使用している場合、*DNS*要求はドロップされ、脅威解析に不可欠な不完全なトラフィック ログの詳細が生成されます。これらのインスタンスでは、次のシンクホール*IP*アドレスを使用する必要があります。*(72.5.65.111)*。

Sinkhole IPv4 (シンクホール **IPv4)** あるいは**Sinkhole IPv6 (**シンクホール **IPv6)** アドレスをネットワーク上のローカル サーバーあるいはループバック アドレスに変更する場合はネットワーク上のローカル サーバーにシンクホールIPアドレスを設定をご覧ください。

9. **OK** をクリックし、アンチスパイウェア プロファイルを保存します。



STEP 5 | アンチスパイウェア プロファイルをセキュリティポリシールールに適用します。

1. **Policies**（ポリシー） > **Security**（セキュリティ）の順に選択します。
2. **Security Policy Rule (**セキュリティポリシー ルール**)** を選択するか、作成します。
3. **Actions (**アクション**)**タブで、**Log at Session End (**セッション終了時にログを記録**)**チェック ボックスをオンにして、ログを有効にします。
4. Profile Setting [プロファイル設定]セクションで**Profile Type**[プロファイルタイプ]ドロップダウンリストをクリックし、すべての**Profiles**[プロファイル]を表示します。**Anti-Spyware (**アンチスパイウェア**)** ドロップダウンリストで、新しい、あるいは修正したプロファイルを選択します。
5. **[OK]** をクリックしてポリシー ルールを保存します。

STEP 6 | ポリシー アクションが適用されているかどうかテストします。

1. DNSセキュリティのテスト ドメインにアクセスして、特定の脅威タイプのポリシー アクションが実施されていることを確認します。
2. ファイアウォール上のアクティビティを監視するには：
   1. 脅威のアクティビティを表示し、アクセスしたドメインのURLテスト ドメインとブロックされたアクティビティを検索します。
   2. **Monitor (**監視**)** > **Logs (**ログ**)** > **Threat (**脅威**)** を選択し、`(action eq sinkhole)` でフィルタリングしてシンクホールされたドメインのログを確認します。
   3. その他のモニタリング オプションについては、DNSセキュリティ サブスクリプション サービスの監視を参照してください。

STEP 7 | オプション: DNS-over-TLS/ポート853トラフィックを復号化する復号ポリシー ルールを作成します。復号化されたDNSペイロードは、DNSポリシー設定を含むアンチスパイウェア プロファイル設定を使用して処理できます。TLSトラフィックを介したDNSセキュリティが復号化されると、脅威ログに記録されるDNS要求は送信元ポートが853の従来のdnsベースのアプリケーションとして表示されます。

STEP 8 | オプション: 悪意のあるドメインへの接続を試みた感染ホストを確認

Advanced DNSセキュリティの有効化

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced DNSセキュリティ ライセンス (拡張機能のサポート用) ❑ Advanced Threat PreventionまたはThreat Preventionライセンス

Advanced DNSセキュリティは、既存のDNSセキュリティ設定を補足し、DNS応答に対する変更を検査することで、DNSハイジャックに対する追加保護を提供します。この手順に進む前に、DNSセキュリティ設定を完全に構成しておく必要があります。

Advanced DNSセキュリティを有効にするには、Advanced DNSセキュリティ サービスにアクセスするためのアンチスパイウェア セキュリティ プロファイルを作成 (または変更) し、DNSシグネチャ カテゴリー(複数可) のログ重大度とポリシー設定を構成し、プロファイルをセキュリティ ポリシー ルールにアタッチする必要があります。

- PAN-OS 11.2以降
- クラウド管理

Advanced DNSセキュリティの有効化（Strata Cloud Manager）

STEP 1 | Palo Alto Networksのサポート アカウントに関連付けられた資格情報を使用し、ハブ上のStrata Cloud Managerにログインします。

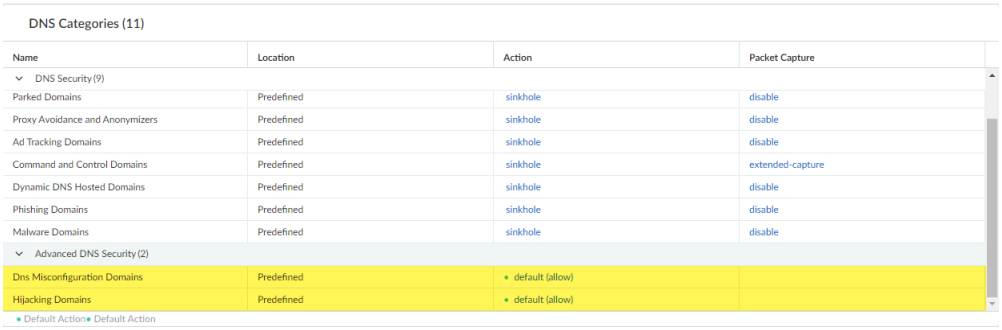
STEP 2 | DNSセキュリティとThreat Preventionのライセンスがアクティブであることを確認します。**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFW]Prisma Access** > **[Overview (概要)]**を選択し、**[License (ライセンス)]**パネルのライセンス使用条件のリンクをクリックします。次のセキュリティ サービスの横に緑色のチェック マークが表示されます。アンチウイルス、アンチスパイウェア、脆弱性防御、DNSセキュリティ。

STEP 3 | リアルタイムのAdvanced DNSセキュリティ クエリを有効にするには、DNSセキュリティ プロファイルを更新または新規作成します。通常、これはDNSセキュリティ設定に使用される既存のDNSセキュリティ プロファイルです。

1. 既存のDNSセキュリティ プロファイルを選択するか、新しいプロファイルを追加します **([Manage (管理)]** > **[Configuration (設定)]** > **[NGFW and Prisma Access (NGFW** およ

び**Prisma Access)]** > **[Security Services (**セキュリティ サービス**)]** > **[DNS Security (DNS**セキュリティ**)]**)。

2. DNSセキュリティ プロファイルを選択し、**[DNS Categories (DNS**カテゴリー**)]**に移動します。



3. Advanced DNSセキュリティ ドメイン カテゴリーごとに、対応するドメイン タイプが検出された場合に実行するポリシーアクションを指定します。現在、2つの解析エンジンが利用可能です:**[DNS Misconfiguration Domains (DNS**の設定ミス ドメイン**)]**と**[Hijacking Domain (**乗っ取りドメイン**)]**です。

   ポリシー アクション オプション**:**

   - **[allow (**許可**)]**: DNSクエリが許可されます。

     許可するアクションとログの重大度を情報に設定することで、該当するドメイン タイプが検出されたときにアラートを生成するようにファイアウォール*Strata Cloud Manager*設定できます。

   - **[block (**ブロック**)]**: DNSクエリがブロックされます。
   - **[sinkhole (**シンクホール**)]**: 検出された悪意のあるドメインを対象とする DNSクエリのDNS応答を作成します。これにより、悪意のあるドメイン名の解決を特定のIPアドレス（シンクホールIPと呼ばれる）に誘導し、応答として埋め込みます。デフォルトのシンクホールIPアドレスはPalo Alto Networksサーバーにアクセスするよう設定されています。Palo Alto Networksはコンテンツ更新によりこのIPアドレスを自動的に更新する場合があります。

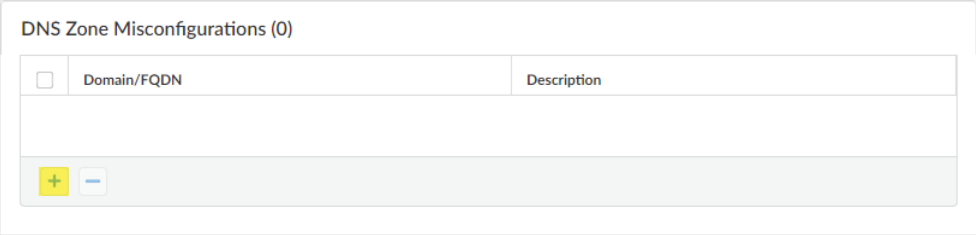
STEP 4 | （任意）組織内で、Advance DNSセキュリティで分析および監視し、誤って設定されたドメインがないかどうかを調べる、パブリックの親ドメインを指定します。誤って設定されたドメインは、CNAME、MX、NSレコード タイプを使用してエイリアス レコードをサードパーティのドメインにポイントするドメイン オーナーによって、無効になったエントリを

使用して不注意に作成され、期限切れまたは未使用のドメインを登録することで攻撃者がドメインを乗っ取ることを可能にします。

TLD（トップレベル ドメイン）とルート レベル ドメインは、*DNS*ゾーンの設定ミス リストに追加できません。

1. Advanced DNSセキュリティ設定を含むDNSセキュリティ プロファイルを選択します**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFW and Prisma Access (NGFW およびPrisma Access)]** > **[Security Services (セキュリティ サービス)]** > **[DNS Security (DNSセキュリティ)]**。
2. **[DNS Zone Miscofigurations (DNSゾーンの設定ミス)]**セクションでは、組織内でのドメインの使用または所有権の特定に役立つ説明をオプションでつけてパブリック向けの親ドメインを追加します。

   エントリには、ドメインに「.」が含まれ、次の形式（例：*paloaltonetworks.com*）を使用している必要があります。含まれていない場合、ホスト名として解析され、プライベート ドメインと見なされます。

3. **[OK]** をクリックして終了し、DNSセキュリティのセキュリティ プロファイルを保存します。

STEP 5 | （オプション）Strata Cloud Manager上のアクティビティを監視し、Advanced DNSセキュリティを使用して検出されたDNSクエリがないか確認します。DNS応答パケットのAdvanced DNSセキュリティのリアルタイム解析のDNSセキュリティ カテゴリーには、プリフィックス「adns」の後にカテゴリが付けられます。たとえば、adns-dnsmisconfigの場合、「dnsmisconfig」はサポートされているDNSカテゴリーの種類を示します。DNS要求パケットを解析してDNSドメインのカテゴリーが決定された場合、指定したカテゴリーはプリフィックス「dns」の後にカテゴリーを付けて表示されます。たとえば 、「dns-grayware」のようになります。

1. Advanced DNSセキュリティのテスト ドメインにアクセスして、特定の脅威タイプのポリシー アクションが実施されていることを確認します。
2. **[Incidents & Alerts (インシデントとアラート)]** > **[Log Viewer (ログビューアー]**を選択します。脅威ログは特定の種類のAdvanced DNSセキュリティ ドメイン カテゴリーに基づいてフィルタにかけることができます。たとえば、`threat_category.value = 'adns-hijacking'`の場合、変数`adns-hijacking`は、Advanced DNSセキュリティ

によって悪意あるDNSハイジャックの試みとして分類されたDNSクエリを示します。ログで使用可能なAdvanced DNSセキュリティの脅威カテゴリーは次のとおりです。

高度DNSセキュリティカテゴリ

- **[DNS Hijacking (DNS**ハイジャック**)]**—`adns-hijacking`

  DNSハイジャック　ドメインの脅威IDは(UTID:109,004,100)。

- **DNS Misconfiguration (DNS**設定ミス**)**:`adns-dnsmisconfig`

  DNS設定ミス ドメインには3つの脅威IDがあり、以下のDNS誤設定ドメインの3つのタイプに対応します: dnsmisconfig_zone（UTID:109,004,200)、dnsmisconfig_zone_dangling (UTID:109,004,201)、dnsmisconfig_claimable_nx (UTID:109,004,202)。特定のDNS設定ミス ドメイン タイプに対応するThreat-ID値を相互参照することで、検索を制限できます。たとえば、`threat_category.value = 'adns-dnsmisconfig'`と`Threat ID = 109004200`です。109004200は、DNSサーバの設定上の問題によりトラフィックをアクティブなドメインにルーティングしないDNSの設定ミス ドメインのThreat IDを示します。

Advanced DNSセキュリティの拡張応答解析を使用して分析されたDNSカテゴリー。

- **DNS**: `adns-benign`
- マルウェア ドメイン: `adns-malware`
- コマンド アンド コントロール ドメイン: `adns-c2`
- フィッシング ドメイン—`adns-phishing`
- ダイナミック**DNS**ホスト ドメイン: `adns-ddns`
- 新規登録ドメイン: `adns-new-domain`
- グレイウェア ドメイン: `adns-grayware`
- パーク ドメイン: `adns-parked`
- プロキシ回避とアノニマイザー: `adns-proxy`
- 広告トラッキング ドメイン: `adns-adtracking`

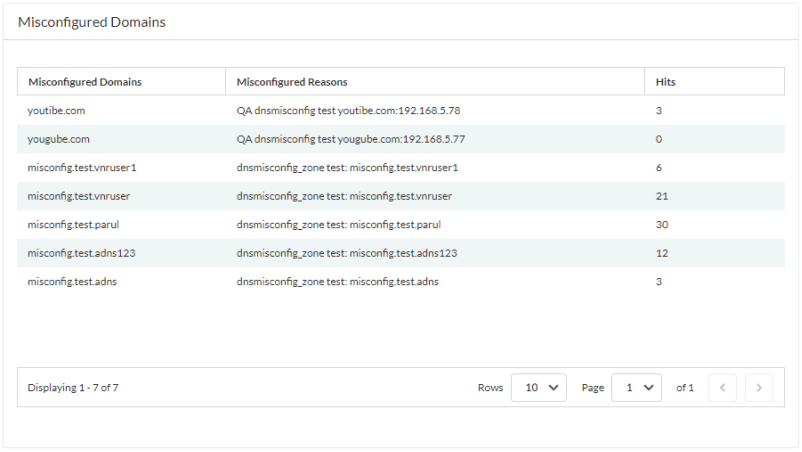
> *DNS*クエリが*Advanced DNS*セキュリティに指定されたタイムアウト時間内に完了しない場合、可能な場合は*DNS*セキュリティ カテゴリーが使用されます。それらのインスタンスでは、カテゴリーのレガシー表記が使用され、たとえば、*`adns-malware`*の代わりに*`dns-malware`*に分類され、*DNS*セキュリティの分類値が使用されたことを示します。

3. DNSクエリの詳細を表示するには、ログ エントリを選択します。
4. DNSカテゴリーは、詳細ログ ビューの **[General (**全般**)]** ペインの下に表示されます。さらに、元のURL、特定の脅威の種類、関連する特性など、脅威のその他の側面を確認することもできます。

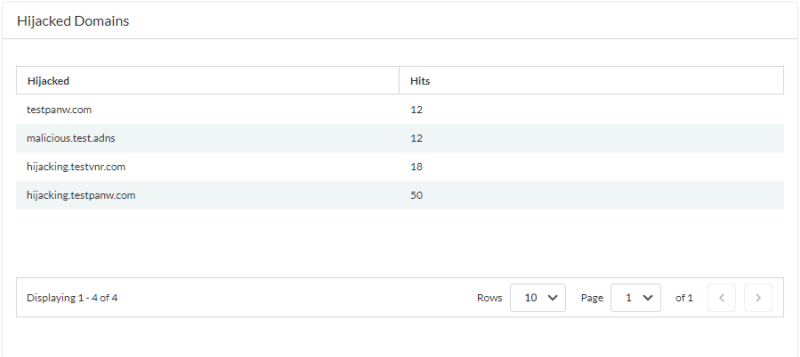
STEP 6 | (オプション)Advanced DNSセキュリティ サービスで検出された、誤って設定されたドメインとハイジャックされたドメインのリストを取得します。正しく構成されていないドメインは、**[DNS Zone Misconfigurations (DNS**ゾーンの設定ミス**)]**に追加されたパブリック向けの親ドメイン エントリに基づいています。

ネットワークから削除されたドメイン エントリの設定ミスは、*Advanced DNS*セキュリティ ダッシュボードの統計情報にすぐには反映されません。

1. Palo Alto Networksのサポート アカウントに関連付けられた資格情報を使用し、ハブ上のStrata Cloud Managerにログインします。
2. **[Dashboard (**ダッシュボード**)]** > **[More Dashboards (**その他のダッシュボード**)]** > **[DNS Security (DNS**セキュリティ**)]**を選択し、DNSセキュリティ ダッシュボードを開きます。
3. DNSセキュリティ ダッシュボードから、次のウィジェットを参照してください。
   - **[Misconfigured Domains (**設定ミス ドメイン**)]**: ユーザー指定のパブリック向け親ドメインに関連付けられた解決不能ドメインのリストを表示します。エントリごとに、設定ミスの理由と、送信元IPに基づくトラフィック ヒット数があります。



   - **[Hijacked Domains (**ハイジャックされたドメイン**)]**: Advanced DNSセキュリティによって決定されたハイジャックされたドメインのリストを表示します。エントリごとに、送信元IPに基づいた分類理由とトラフィック ヒット数があります。



Advanced DNSセキュリティの有効化（PAN-OS 11.2以降）

Palo Alto Networksは、DNSセキュリティ機能を有効にしてから、Advanced DNSセキュリティをセットアップすることをお勧めします。

STEP 1 | NGFWにログインします。

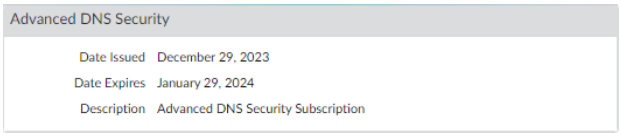
STEP 2 | コンテンツ リリースバージョンを8832以降に更新します。

STEP 3 | Advanced DNSセキュリティを使用して既知および未知の悪意のあるドメインへのアクセスを防ぐには、Advanced DNSセキュリティのライセンスがアクティブである必要があります。これはPAN-OS 11.2にアップグレードした後にのみインストールしてください。

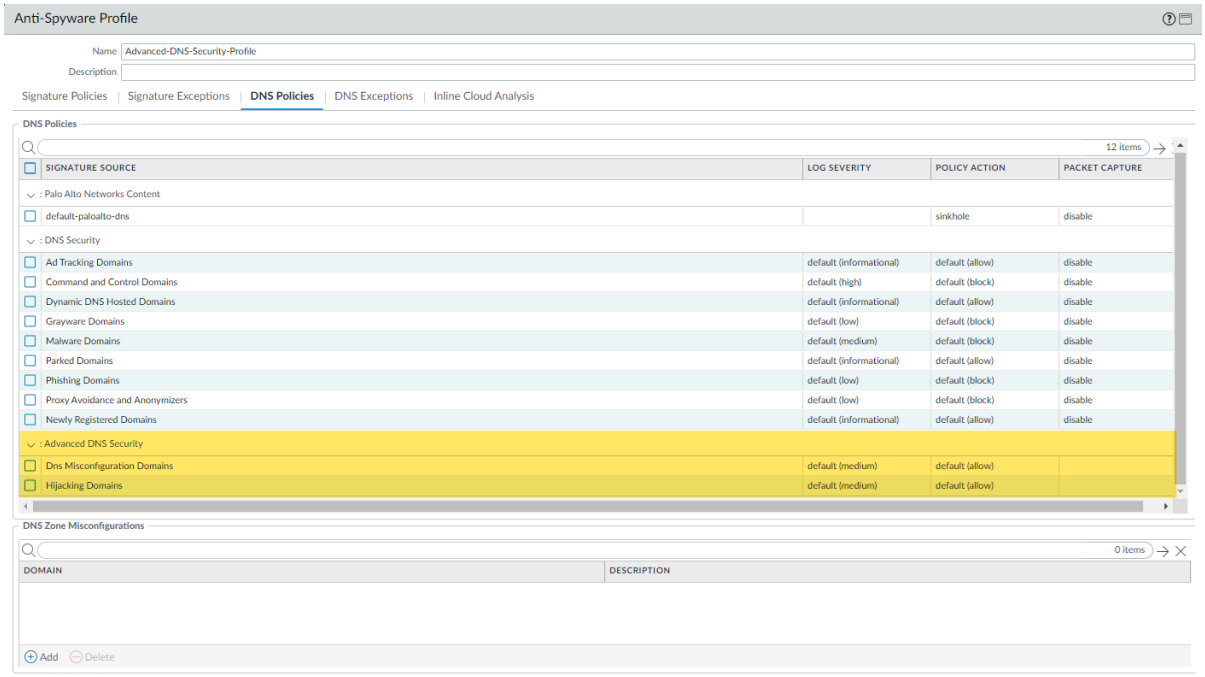
*Advanced DNS*セキュリティは、以前にライセンス供与されていなかったファイアウォールにインストールした場合に、*DNS*セキュリティの機能を*Advanced DNS*セキュリティ ライセンスに包含するライセンス モデルをサポートします。既存の*DNS*セキュリティ ライセンスを持つファイアウォールからアップグレードする場合は、個別の*DNS*セキュリティ ライセンスと *Advanced DNS*セキュリティ ライセンスが存在することを示すエントリが表示されます。この場合、*DNS*セキュリティ ライセンスはパッシブ エントリであり、関連する有効期限を含め、すべての*DNS*セキュリティおよび*Advanced DNS*セキュリティ機能は*Advanced DNS*ライセンスを通じて付与されます。以前にインストールされた*DNS*セキュリティ ライセンスのないファイアウォールでは、*Advanced DNS*セキュリティ ライセンスが表示されますが、*DNS*セキュリティと*Advanced DNS*セキュリティの両方の機能を提供します。

そのため、*Advanced DNS*セキュリティ ライセンスを運用している *PAN-OS*リリースから*Advanced DNS*セキュリティをサポートしていないリリースにダウングレードした場合、ファイアウォールは引き続き*Advanced DNS*セキュリティ ライセンスを通じて*DNS*セキュリティ機能を表示し、付与します。ただし、基本的な*DNS*セキュリティ機能に限定されます。

現在アクティブなライセンスがあるサブスクリプションを確認するには、**[Device (**デバイス**)]) > [Licenses (**ライセンス**)]**を選択し、適切なライセンスが使用可能で有効期限が切れていないことを確認します。



STEP 4 | アンチスパイウェア セキュリティ プロファイルを更新または新規作成して、リアルタイムのAdvanced DNSセキュリティ クエリを有効にします。通常、これはDNSセキュリティ設定に使用される既存のアンチスパイウェア セキュリティ プロファイルです。



1. 既存のアンチスパイウェア セキュリティ プロファイルを選択するか、新しいセキュリティ プロファイルを**[Add (追加)]**します (**[Object (オブジェクト)]** > **[Security Profiles (セキュリティ プロファイル)]** > **[Anti-Spyware (アンチスパイウェア)]**)。
2. アンチスパイウェア セキュリティ プロファイルを選択し、**[DNS Policies (DNSポリシー)]**に移動します。
3. Advanced DNSセキュリティ ドメイン カテゴリーごとに、対応する解析エンジンを使用してドメイン タイプが検出された場合に実行する**[Log Severity (ログ重大度)]**と**[Policy Action (ポリシー アクション)]**を指定します。現在、次の2つの解析エンジンを利用できます。**[DNS Misconfiguration Domains (DNSの設定ミス ドメイン)]**と**[Hijacking Domain (乗っ取りドメイン)]**です。

   ポリシー アクション オプション**:**

   - **[allow (許可)]**: DNSクエリが許可されます。

     許可するアクションとログの重大度を情報に設定することで、該当するドメイン タイプが検出されたときにアラートを生成するようにファイアウォールを設定できます。

   - **[block (ブロック)]**: DNSクエリはブロックされます。
   - **[sinkhole (シンクホール)]**: 検出された悪意のあるドメインを対象とするDNSクエリのDNS応答を作成します。これにより、悪意のあるドメイン名の解決を特定のIPアドレス（シンクホールIPと呼ばれる）に誘導し、応答として埋め込みます。デフォルトのシ

ンクホールIPアドレスはPalo Alto Networksサーバーにアクセスするよう設定されています。Palo Alto Networksはコンテンツ更新によりこのIPアドレスを自動的に更新する場合があります。

ログの重大度オプション:

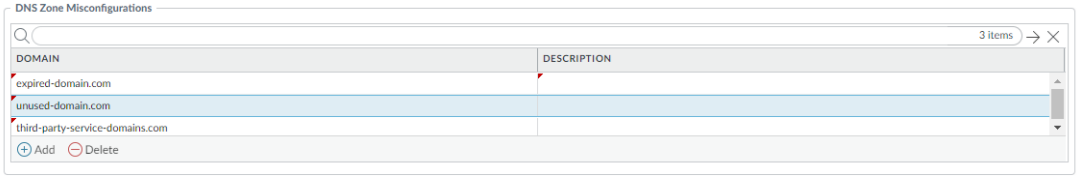
- **none**: イベントにログ重大度が関連付けられていません。
- **low**: 組織のインフラストラクチャへの影響がわずかな警告レベルの脅威。通常、ローカルまたは物理的なシステムへのアクセスが必要であり、被害者のプライバシーや DoS の問題、情報漏洩などが発生することがあります。
- **[informational (情報)]**: 直ちに脅威とはならなくても、存在する可能性がある深層の問題に注意を引くために報告される、疑わしいイベント。
- **[medium (中)]**: 影響が最小限に抑えられる小さな脅威。たとえば、標的に侵入することのないDoS攻撃や、攻撃者が被害サーバーと同じLAN上に存在する必要があり、標準以外の設定や隠れたアプリケーションにのみ影響するか、アクセスがごく限られている悪用などです。
- **[high (高)]**: 重大度が[critical (重大)] に変わる可能性があるものの、軽減要因が存在する脅威。たとえば、悪用するのが困難であったり、上位の特権が与えられることがなかったり、被害サーバー数が多くなかったりする場合です。
- **[critical (重大)]**: 広範囲にデプロイされたソフトウェアのデフォルト インストールに影響するような深刻な脅威。サーバーのrootが悪用され、弱点のあるコードが広範囲の攻撃者の手に渡ることになります。攻撃者は通常、特殊な認証資格証明や個々の被害者に関する知識を必要としません。また、標的がなんらかの特殊な機能を実行するように操作する必要もありません。

4. **[OK]** をクリックしてアンチスパイウェア セキュリティ プロファイル設定ダイアログを終了し、**[Commit (コミット)]** をクリックして変更を行います。

STEP 5 | （任意）組織内で、Advance DNSセキュリティで分析および監視し、誤って設定されたドメインがないかどうかを調べる、パブリックの親ドメインを指定します。誤って設定されたドメインは、CNAME、MX、NSレコード タイプを使用してエイリアス レコードをサードパーティのドメインにポイントするドメイン オーナーによって、無効になったエントリを

使用して不注意に作成されるもので、期限切れまたは未使用のドメインを登録することで攻撃者がドメインを乗っ取ることを可能にします。

TLD（トップレベル ドメイン）とルート レベル ドメインは、*DNS*ゾーンの設定ミス リストに追加できません。



1. アンチスパイウェア セキュリティ プロファイル(**[Objects (オブジェクト)]** > **[Security Profiles (セキュリティ プロファイル)]** > **[Anti-Spyware (アンチスパイウェア)]**）を選択し、**[DNS Policies (DNSポリシー)]**に移動します。
2. **[DNS Zone Miscofigurations (DNSゾーンの設定ミス)]]**セクションでは、組織内でのドメインの使用または所有権の特定に役立つ説明をオプションでつけてパブリック向けの親ドメインを追加します。

   エントリには、ドメインに「.」が含まれ、次の形式（例：*paloaltonetworks.com*）を使用している必要があります。含まれていない場合、ホスト名として解析され、プライベート ドメインと見なされます。
3. **[OK]** をクリックしてアンチスパイウェア セキュリティ プロファイル設定ダイアログを終了し、**[Commit (コミット)]** をクリックして変更を行います。

STEP 6 | （オプション）Advanced DNSシグネチャ検索の最大タイムアウト設定を行います。この値を超えると、Advanced DNSセキュリティを使用して解析を実行せずにDNS応答が通過します。

STEP 7 | （オプション［最新のデバイス証明書がない場合］）Advanced Threat Preventionインライン クラウド分析サービスへの認証に使用する、更新されたファイアウォール デバイス証明書をインストールしますインラインクラウド解析が有効なすべてのファイアウォールについて繰り返します。

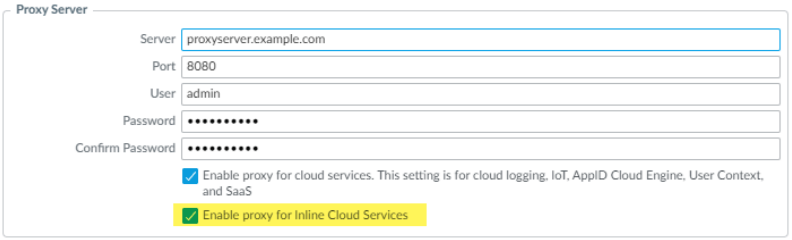
IoT Security、Device Telemetry、Advanced Threat Prevention、Advanced URL Filteringのオンボーディング プロセスの一部として、更新されたファイアウォール デバイス証明書をすでにインストールしている場合は、この手順は必要ありません。

STEP 8 | (ファイアウォールが明示的なプロキシ サーバーを使用してデプロイされている場合に必要)設定されたすべてのインライン クラウド解析機能によって生成される要求を容易にするサーバーへのアクセスに使用するプロキシ サーバーを構成します。単一のプロキシ サー

バーを指定することができ、構成済みのすべてのインライン クラウドおよびロギング サービスを含む、すべてのPalo Alto Networksの更新サービスに適用されます。

1. （PAN-OS 11.2.3以降）PAN-OSを介してプロキシサーバーを構成します。
   1. **[Device (デバイス)]** > **[Setup (セットアップ)]** > **[Services (サービス)]** の順に選択し、**[Services (サービス)]**セクションを編集します。
   2. **[Proxy Server (プロキシ サーバー)]**]設定を指定し、**[Enable proxy for Inline Cloud Services (インライン クラウド サービスのプロキシを有効にする]**を選択します。［**Server (サーバー)**］フィールドにIPアドレスまたは FQDNのいずれかを指定できます。

      プロキシ サーバーのパスワードには、*6*文字以上を含める必要があります。

   3. **OK** をクリックします。

STEP 9 | （任意） Advanced DNSセキュリティ クラウド サービスへのファイアウォール接続のステータスを確認します。

STEP 10 | （オプション）ファイアウォール上のアクティビティを監視し、Advanced DNS セキュリティを使用して検出されたDNSクエリがないか確認します。DNS応答パケットのAdvanced DNSセキュリティのリアルタイム解析のDNSセキュリティ カテゴリーには、プリフィックス「adns」の後にカテゴリが付けられます。たとえば、adns-dnsmisconfigの場合、「dnsmisconfig」はサポートされているDNSカテゴリーの種類を示します。DNS要求パケットを解析してDNSドメインのカテゴリーが決定された場合、指定したカテゴリーはプリフィックス「dns」の後にカテゴリーを付けて表示されます。たとえば 、「dns-grayware」のようになります。

1. Advanced DNS Securityのテスト ドメインにアクセスして、特定の脅威タイプのポリシー アクションが実施されていることを確認します。
2. **[Monitor (監視)]** > **[Logs (ログ)]** > **[Threat (脅威)]**を選択します。ログは特定の種類のAdvanced DNSセキュリティ ドメイン カテゴリーに基づいてフィルタにかけることができます。たとえば、`(category-of-threatid eq adns-hijacking )`の場合、変数`adns-hijacking`は、Advanced DNSセキュリティによって悪意あるDNSハイ

ジャックの試みとして分類されたDNSクエリを示します。ログで使用可能なAdvanced DNSセキュリティの脅威カテゴリーは次のとおりです。

高度DNSセキュリティカテゴリ

- **[DNS Hijacking (DNS**ハイジャック**)]**—`adns-hijacking`

  DNSハイジャック　ドメインの脅威IDは(UTID:109,004,100)。

- **DNS Misconfiguration (DNS**設定ミス**)**:`adns-dnsmisconfig`

  DNS設定ミス ドメインには3つの脅威IDがあり、以下のDNS誤設定ドメインの3つのタイプに対応します: dnsmisconfig_zone（UTID:109,004,200)、dnsmisconfig_zone_dangling (UTID:109,004,201)、dnsmisconfig_claimable_nx (UTID:109,004,202)。特定のDNS設定ミス ドメイン タイプに対応するThreat-ID値を相互参照することで、検索を制限できます。たとえば、（category-of-threatid eq adns-dnsmisconfig）と（threatid eq 109004200）です。109004200は、DNSサーバの設定上の問題によりトラフィックをアクティブなドメインにルーティングしないDNSの設定ミス ドメインのThreat IDを示します。

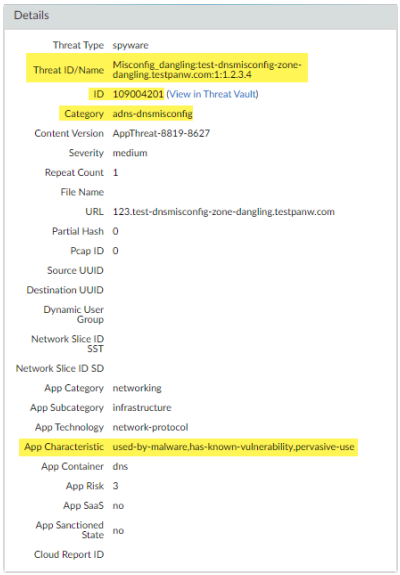
Advanced DNS Securityの拡張応答解析を使用して分析されたDNSカテゴリー。

> 拡張された*Advanced DNS*セキュリティのリアルタイム解析を利用するには、*PAN-OS 11.2*以降を実行するファイアウォールを運用する必要があります。

- **DNS**: `adns-benign`
- マルウェア ドメイン: `adns-malware`
- コマンド アンド コントロール ドメイン: `adns-c2`
- フィッシング ドメイン: `adns-phishing`
- ダイナミック**DNS**ホスト ドメイン: `adns-ddns`
- 新規登録ドメイン: `adns-new-domain`
- グレイウェア ドメイン: `adns-grayware`
- パーク ドメイン: `adns-parked`
- プロキシ回避とアノニマイザー: `adns-proxy`
- 広告トラッキング ドメイン: `adns-adtracking`

> *DNS*クエリが*Advanced DNS*セキュリティに指定されたタイムアウト時間内に完了しない場合、可能な場合は*DNS*セキュリティ カテゴリーが使用されます。それらのインスタンスでは、カテゴリーのレガシー表記が使用され、たとえば、*`adns-malware`*の代わりに*`dns-malware`*に分類され、*DNS*セキュリティの分類値が使用されたことを示します。

3. DNSクエリの詳細を表示するには、ログ エントリを選択します。
4. DNSカテゴリーは、詳細ログ ビューの**[Details (詳細)]**ペインの下に表示されます。さらに、発信元ドメイン、特定の脅威カテゴリー、およびその他の関連する特性を含む脅威ID、および関連するQタイプ、ハイジャック:<FQDN>:<QTYPE>:<RDATA>の形式を使用したRデータなど、脅威の他の側面を確認できます。ここで、<QTYPE>はDNSリソース レコードの種類、<RDATA>はハイジャックされたIPアドレスを表します。

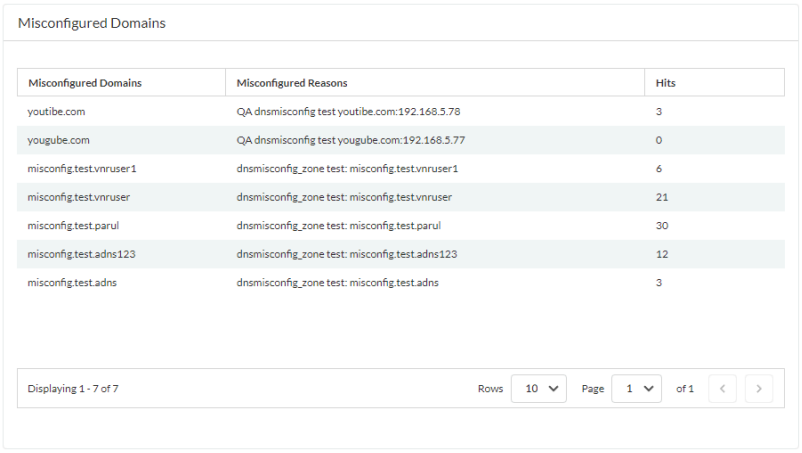


STEP 11 | (オプション)Advanced DNSセキュリティ サービスで検出された、誤って設定されたドメインとハイジャックされたドメインのリストを取得します。正しく構成されていないドメイ

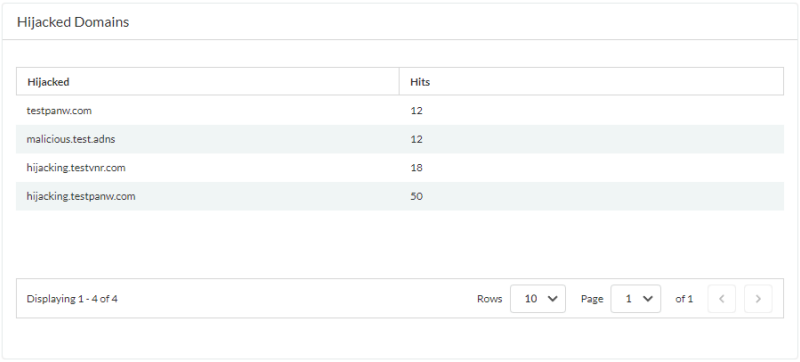
ンは、**[DNS Zone Misconfigurations (DNSゾーンの設定ミス)]**に追加されたパブリック向けの親ドメイン エントリに基づいています。

ネットワークから削除されたドメイン エントリの設定ミスは、*Advanced DNS*セキュリティ ダッシュボードの統計情報にすぐには反映されません。

1. Palo Alto Networksのサポート アカウントに関連付けられた資格情報を使用し、ハブ上のStrata Cloud Managerにログインします。
2. **[Dashboard (ダッシュボード)]** > **[More Dashboards (その他のダッシュボード)]** > **[DNS Security (DNSセキュリティ)]**を選択し、DNSセキュリティ ダッシュボードを開きます。
3. DNSセキュリティ ダッシュボードから、次のウィジェットを参照してください。
   - **[Misconfigured Domains (設定ミス ドメイン)]**: ユーザー指定のパブリック向け親ドメインに関連付けられた解決不能ドメインのリストを表示します。エントリごとに、設定ミスの理由と、送信元IPに基づくトラフィック ヒット数があります。



   - **[Hijacked Domains (ハイジャックされたドメイン)]**: Advanced DNSセキュリティによって決定されたハイジャックされたドメインのリストを表示します。エントリごとに、送信元IPに基づいた分類理由とトラフィック ヒット数があります。



TLSを介したDNSセキュリティの設定

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced DNSセキュリティ ライセンス（拡張機能サポート用）またはDNSセキュリティ ライセンス ❑ Advanced Threat PreventionまたはThreat Preventionライセンス

暗号化されたDNS要求に含まれるDNSペイロードを復号化することで、TLS要求を介したDNSセキュリティの可視化と制御が可能になります。復号化されたDNSペイロードは、DNSポリシー設定を含むセキュリティ プロファイル設定を使用して処理できます。TLS送信元であると判定されたDNS要求は、脅威ログに送信元ポート853が記録されます。

- Strata Cloud Manager
- PAN-OS & Panorama

TLSを介したDNSセキュリティの設定 (Strata Cloud Manager)

STEP 1 | Palo Alto Networksのサポート アカウントに関連付けられた資格情報を使用し、ハブ上のStrata Cloud Managerアプリケーションにログインします。

STEP 2 | DNS セキュリティの有効化はDNS要求を検査するように設定されています。TLSトラフィックを介したDNSセキュリティに同じ**DNS**ポリシー 設定を使用する場合は、既存のセキュリティ プロファイルを使用できます。

STEP 3 | TLSトラフィックを介したDNSセキュリティ含む、ポート853のHTTPSトラフィックを復号化するアクションを含む復号ポリシー ルールを作成します（詳細については、復号化ベストプラクティスを参照してください）。TLSトラフィックを介したDNSセキュリティが復号化されると、ログに記録されるDNS要求は従来の**dns**ベースのアプリケーションとして表示されます。

STEP 4 | （オプション）DNSセキュリティを使用して処理され、復号化されたTLS暗号化DNSクエリのファイアウォール上のアクティビティを検索します。

1. **[Activity (アクティビティ)]** > **[Log Viewer (ログ ビューワー)]**を選択し、**[Threat (脅威)]**ログを選択します。クエリ ビルダーを使用して、**dns-base**とポート853（TLS トランザクション経由のDNSセキュリティ専用）を使用するアプリケーションに基づい

てフィルタリングします。たとえば、`app = 'dns-base' AND source_port = 853`です。

2. ログ エントリを選択して、検出されたDNS脅威の詳細を表示します。
3. **[Application (アプリケーション)]**には、［**General (全般)**］ペインに**dns-base**が表示され、詳細ログ ビューの［**Source (送信元)**］ペインに［**Port (ポート)**］が表示されるはずです。脅威に関するその他の関連詳細は、対応するタブに表示されます。

TLSを介したDNSセキュリティの設定 (NGFW (Managed by PAN-OS or Panorama))

STEP 1 | NGFWにログインします。

STEP 2 | DNS セキュリティの有効化はDNS要求を検査するように設定されています。TLSトラフィックを介したDNSセキュリティに同じ**DNS**ポリシー 設定を使用する場合は、既存のセキュリティ プロファイルを使用できます。

STEP 3 | TLSトラフィックを介したDNSセキュリティ含む、ポート853のHTTPSトラフィックを復号化するアクションを含む復号ポリシー ルールを作成します（詳細は、復号化ベストプラクティスを参照してください）。TLSトラフィックを介したDNSセキュリティが復号化されると、ログに記録されるDNS要求は従来の**dns**ベースのアプリケーションとして表示されます。

		Source				Destination					Decrypt Options					
	NAME	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	URL CATEGORY	SERVICE	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNS SSL HAN
1	Decrypt Port 853	any	any	any	any	any	any	any	any	Port 853	decrypt	ssl-forward-proxy	default	none	false	true

STEP 4 | （オプション）DNSセキュリティを使用して処理され、復号化されたTLS暗号化DNSクエリのファイアウォール上のアクティビティを検索します。

1. **[Monitor (監視する)** > **[Logs (ログ)]** > **[Traffic (トラフィック)]**を選択し、**dns-base**とポート853を(TLSトランザクションを介したDNSセキュリティにのみ使用)、例えば`(app eq dns-base)`や`(port.src eq 853)`のように使用するアプリケーションに基づいてフィルタをかけます。
2. ログ エントリを選択して、検出されたDNS脅威の詳細を表示します。
3. **[Application (アプリケーション)]**には、［**General (全般)**］ペインに**dns-base**が表示され、詳細ログ ビューの［**Source (送信元)**］ペインに［**Port (ポート)**］が表示されるはずです。脅威に関するその他の関連詳細は、対応するウィンドウに表示されます。

DoHによるDNSセキュリティの設定

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced DNSセキュリティ ライセンス（拡張機能サポート用）またはDNSセキュリティ ライセンス ❑ Advanced Threat PreventionまたはThreat Preventionライセンス

HTTPS (DoH—[DNS-over-HTTPS])を使用して、暗号化されたDNSトラフィック要求に含まれるDNSペイロードを分析し、分類できます。現在、Palo Alto Networksが推奨するすべてのDoH要求をブロックしている組織であれば、DNSセキュリティによって暗号化されたリクエストからDNSホスト名を抽出し、組織の既存のDNSセキュリティポリシーを適用できるようになったため、そのポリシーから移行することができます。これにより、DoHのサポートが広がるにつれて、より多くのウェブサイトに安全にアクセスできるようになります。DoHに対するDNSセキュリティのサポートは、ユーザーが指定したDNSリゾルバーのリストを起点とするDNS要求のペイロードを復号化するようにファイアウォールを設定することで有効になり、多くのサーバー オプションのサポートを提供します。復号化されたDNSペイロードは、DNSポリシー設定を含むアンチスパイウェア プロファイル設定を使用して処理できます。DoHと判定されたDNS要求は、トラフィック ログに**dns-over-https**とラベル付けされます。

- Strata Cloud Manager
- PAN-OS 11.0以降

DoH（Strata Cloud Manager）を介したDNSセキュリティの設定

STEP 1 | Palo Alto Networksのサポート アカウントに関連付けられた資格情報を使用し、ハブ上のStrata Cloud Managerにログインします。

STEP 2 | トラフィックを送受信できるようにするすべてのDoHリゾルバーを含むカスタムURLカテゴリー リストを作成します（DNSサーバーのURLが必要です）。

STEP 3 | 前のステップで作成したカスタムURLカテゴリー リストを参照する復号ポリシー ルールを作成します。

STEP 4 | DoH要求の検査に使用するアンチスパイウェア セキュリティ プロファイルを更新または新規作成します。

STEP 5 | セキュリティ ポリシー ルールを作成または更新し、DoHサーバーの承認済みリストを含むDNSセキュリティ プロファイルとカスタムURLカテゴリー リスト（**[Manage (管理)]** > **[Configuration (設定)]** > **[PAN-OS and Prisma Access(PAN-OSとPrisma Access)]** > **[Security Services (セキュリティ サービス)]** > **[URL Access Management (URLアクセス管理)]**)を参照します。

STEP 6 | App-ID: **dns-over-https**とURLカテゴリー: **encrypted-dns**を使用して、HTTPSトラフィックを復号化し、カスタムURLカテゴリー リスト（手順5で参照）で明示的に許可されていない残りのすべての非認可DoHトラフィックをブロックするブロック ポリシーを作成します。

> *DoH*トラフィックをブロックする既存のブロック ポリシーがある場合は、カスタム*URL*カテゴリー リスト オブジェクトにリストされている特定の*DoH*リゾルバーとのマッチングに使用される以前のセキュリティ ポリシー ルールの下にルールが配置されることを確認します。

STEP 7 | （オプション）DNSセキュリティを使用して処理されたHTTPS暗号化DNSクエリのファイアウォール上のアクティビティを検索します。

1. **[Activity (アクティビティ)]** > **[Logs (ログ)]** > **[Log Viewer (ログ ビューワー)]**、**[Threat (脅威)]**を選択します
2. **dns-over-https**を使用して、アプリケーションに基づいたログ クエリを送信します。たとえば、`app = 'dns-over-https'`のように入力します。
3. ログ エントリを選択して、DoHを使用する検出されたDNS脅威の詳細を表示します。
4. 詳細ログ ビューの**[General (全般)]**ペインに脅威の**[Application (アプリケーション)]**が表示されます。脅威に関するその他の関連詳細は、対応するウィンドウに表示されます。

DoHを介したDNSセキュリティの設定（PAN-OS 11.0以降）

STEP 1 | PAN-OS Web インターフェイスにログインします。

STEP 2 | トラフィックを送受信できるようにするすべてのDoHリゾルバーを含むカスタムURLカテゴリーリストを作成します（DNSサーバーのURLが必要です）。

STEP 3 | 前のステップで作成したカスタムURLカテゴリー リストを参照する復号ポリシー ルールを作成します。

STEP 4 | DoH要求の検査に使用するアンチスパイウェア セキュリティ プロファイルを更新または新規作成します。

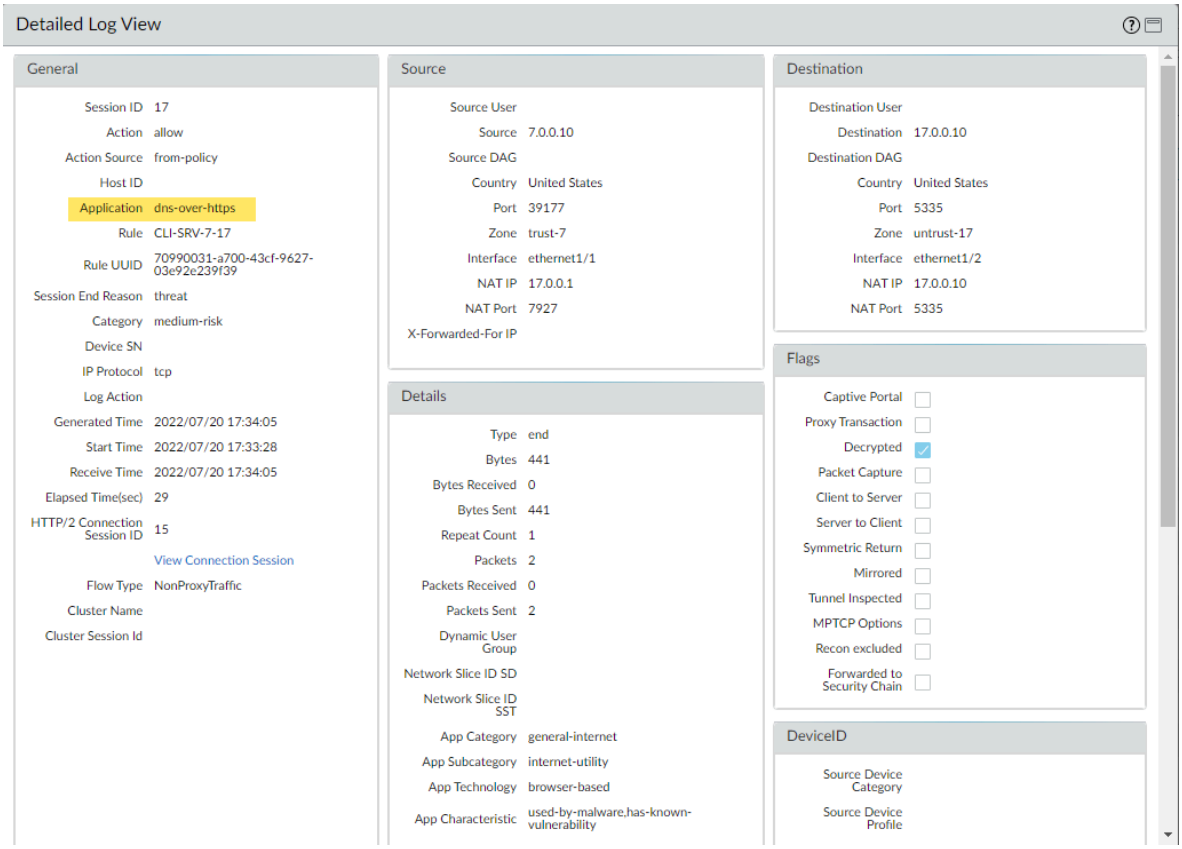
STEP 5 | セキュリティ ポリシー ルール を作成または更新し、DoHサーバーの承認リストを含むアンチスパイウェア プロファイルとカスタムURLカテゴリー リスト（**[Objects (オブジェクト)]** > **Custom Objects (カスタムオブジェクト)** > **[URL Category (URLカテゴリー)]**)を参照します。

STEP 6 | App-ID: **dns-over-https**とURLカテゴリー: **encrypted-dns**を使用して、HTTPSトラフィックを復号化し、カスタムURLカテゴリー リスト（手順5で参照）で明示的に許可されていない残りのすべての非認可DoHトラフィックをブロックするブロック ポリシーを作成します。

*DoH*トラフィックをブロックする既存のブロック ポリシーがある場合は、カスタム*URL*カテゴリー リスト オブジェクトにリストされている特定の*DoH*リゾルバーとのマッチングに使用される以前のセキュリティ ポリシー ルールの下にルールが配置されることを確認します。

STEP 7 | （オプション）DNSセキュリティを使用して処理されたHTTPS暗号化DNSクエリのファイアウォール上のアクティビティを検索します。

1. **[Monitor (監視)]** > **[Logs (ログ)]** > **[Traffic (トラフィック)]** を選択し、**dns-over-https** などを使用してアプリケーションに基づいてフィルタリングします（ `app eq dns-over-https` ）。
2. ログ エントリを選択して、検出されたDNS脅威の詳細を表示します。
3. **[Application (アプリケーション)]**は、詳細ログ ビューの**[General (全般)]**ペインにdns-over-httpsと表示し、これがDNSセキュリティを使用して処理されたDoHトラフィックであることを示します。脅威に関するその他の関連詳細は、対応するウィンドウに表示されます。



ドメイン例外の作成と許可 | ブロックリスト

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced DNSセキュリティ ライセンス（拡張機能サポート用）またはDNSセキュリティ ライセンス ❑ Advanced Threat PreventionまたはThreat Preventionライセンス

DNSセキュリティは、DNSセキュリティ サービスによって分析されたドメインの脅威シグネチャを作成します。これらの既知のドメインでは、DNSクエリを受信するとシグネチャが参照されます。場合によっては、ドメインに存在する特定の機能や性質のために、シグネチャがドメインを脅威として誤って分類している可能性があります。このような場合、シグネチャ例外を追加して、これらの誤検知を回避できます。内部ドメインなど、悪意のあるドメインとして分類されている安全な既知のドメインがある場合は、任意のDNS解析をバイパスするドメインのリストを追加できます。組織が包括的な脅威インテリジェンス ソリューションの一部としてサードパーティの脅威フィードを使用している場合は、DNSセキュリティ プロファイルで外部の動的リスト（EDL）の形でそれらを参照することもできます。

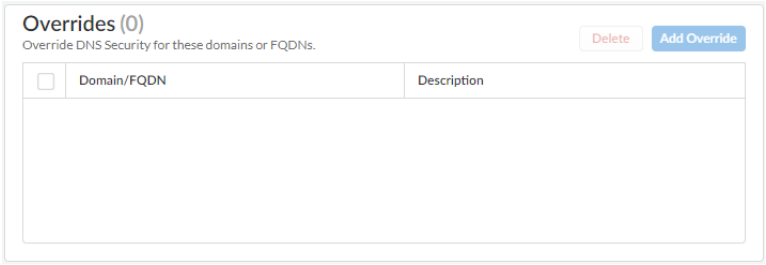
- Strata Cloud Manager
- PAN-OS & Panorama

ドメイン例外の作成と許可 | ブロックリスト(Strata Cloud Manager)

STEP 1 | Palo Alto Networksのサポート アカウントに関連付けられた資格情報を使用し、ハブ上のStrata Cloud Managerにログインします。

STEP 2 | 誤検知が発生した場合にドメイン オーバーライドを追加します。

1. **[Manage (管理)]** > **[Configuration (設定)]** > **[NGFW]Prisma Access** > **[Security Services (セキュリティ サービス)]** > **[DNS Security (DNSセキュリティ)]**を選択し、変更するDNSセキュリティ プロファイルを選択します。
2. 必要に応じてドメイン リストのエントリを変更するには、**[Add Override (オーバーライドの追加)]**または**[Delete (削除)]**をクリックします。エントリを追加するたびに、ドメインと説明が必要です。



3. **[OK]**をクリックして、変更したDNSセキュリティ プロファイルを保存します。

STEP 3 | DNSセキュリティ プロファイルの一部として外部の動的リスト(EDL）を参照し、サードパーティの脅威フィードをインポートします。

1. ドメインベースの外部ダイナミック リストを作成します(**[Manage (管理)]** > **[Configuration (設定)]** > **[NGFW]Prisma Access** > **[Objects (オブジェクト)]** > **External Dynamic Lists (外部ダイナミック リスト)]**)。EDLの詳細については、「外部ダイナミック リスト」を参照してください。
2. **[Manage (管理)]** > **[Configuration (設定)]** > **[NGFW]Prisma Access** > **[Security Services (セキュリティ サービス)]** > **[DNS Security (DNSセキュリティ)]**を選択します。
3. **[External Dynamic Lists (外部ダイナミック リスト)]**パネルで、ドメイン リストEDLを選択し、**[Policy Action (ポリシー アクション)]**と**[Packet Capture (パケット キャプチャ)]**の設定を選択します。**[Apply to Profiles (プロファイルに適用)]**で、EDLドメイン リストを適用するDNSセキュリティ プロファイルを選択します。
4. 更新が終了したら、変更を保存します。

ドメイン例外の作成と許可 | ブロックリスト(NGFW (Managed by PAN-OS or Panorama))

PAN-OS 10.0以降のリリースでは、アンチスパイウェア セキュリティ プロファイルを通じて許可ドメインを明示的に追加する追加オプションが提供されています。承認されたドメイン ソースのドメイン/FQDNエントリがDNSセキュリティからの誤検知応答をトリガーする場合、それらのエントリを追加できます。

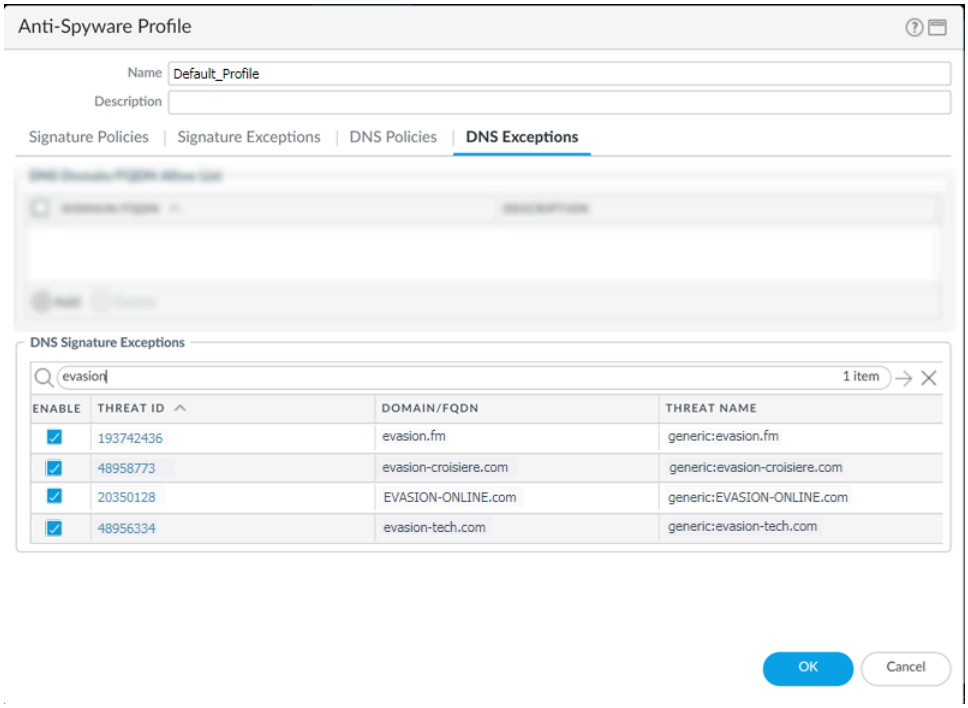
- PAN-OS 10.0 以降
- PAN-OS 9.1

ドメイン例外の作成と許可 | ブロック リスト (PAN-OS 10.0以降)

NGFWにログインします。

誤検知が発生した場合に備えて、ドメイン シグネチャの例外を追加します。

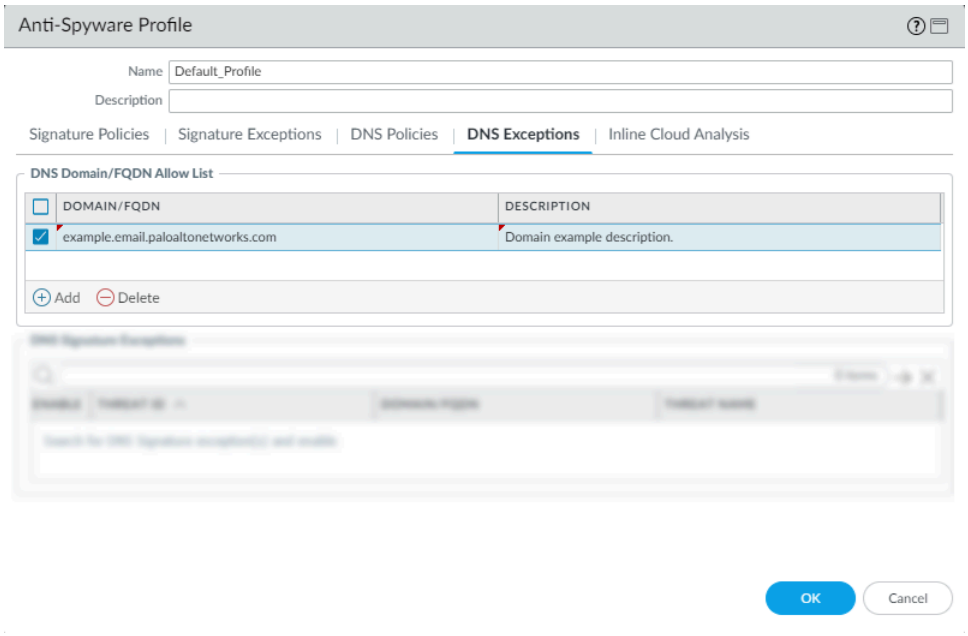
1. **Objects (オブジェクト) > > Security Profiles (セキュリティ プロファイル) > > Anti-Spyware (アンチスパイウェア)** を選択します。
2. 変更するプロファイルを選択します。
3. 脅威シグネチャを除外したいアンチスパイウェア プロファイルを **Add (追加)** するか、既存のものを変更し、**DNSExceptions (DNS 例外)** を選択します。
4. 名前あるいは FQDN を入力し、除外する DNS シグネチャを検索します。
5. 適用から除外する DNSシグネチャの各 **[Threat ID (脅威ID)]**のチェックボックスをオンにします。



6. **OK** をクリックし、新しい、あるいは変更したアンチスパイウェア プロファイルを保存します。

許可リストを追加して、明示的に許可するDNS ドメイン/FQDN のリストを指定します。

1. **Objects (オブジェクト) > > Security Profiles (セキュリティ プロファイル) > > Anti-Spyware (アンチスパイウェア)** を選択します。
2. 変更するプロファイルを選択します。
3. 脅威シグネチャを除外したいアンチスパイウェア プロファイルを **Add (追加)** するか、既存のものを変更し、**DNSExceptions (DNS 例外)** を選択します。
4. 新しい[FQDN Allow List (FQDN 許可リスト)]を**[Add (追加)]**するには、DNSドメインまたはFQDNロケーションおよび説明を指定します。



5. **OK** をクリックし、新しい、あるいは変更したアンチスパイウェア プロファイルを保存します。

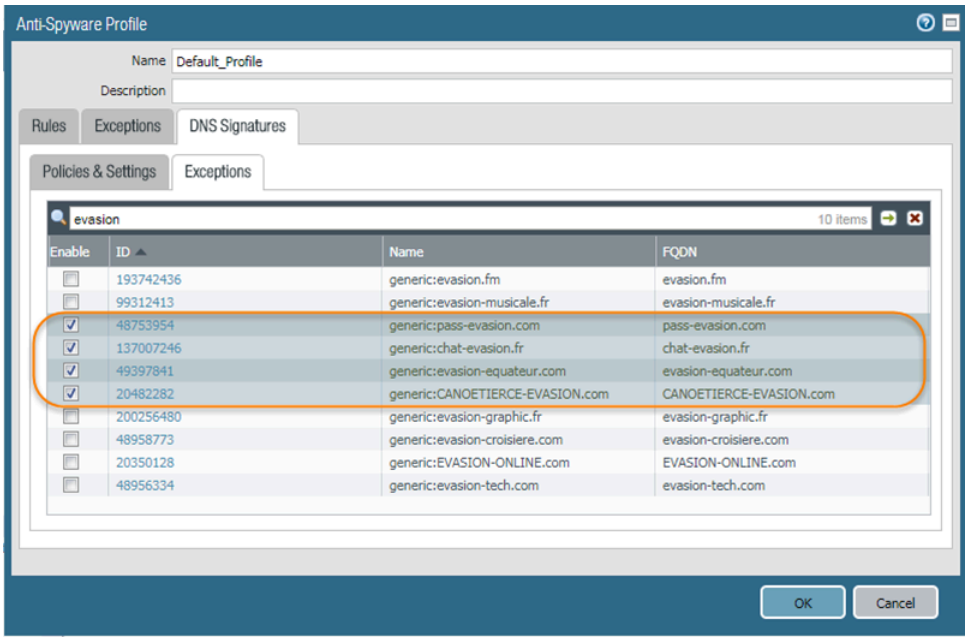
ドメイン例外の作成と許可 | ブロック リスト (PAN-OS 9.1)

許可リストとブロックリストは*PAN-OS 9.1*では使用できません。

NGFWにログインします。

誤検知が発生した場合に備えて、ドメイン シグネチャの例外を追加します。

1. **Objects (**オブジェクト**) > > Security Profiles (**セキュリティ プロファイル**) > > Anti-Spyware (**アンチスパイウェア**)** を選択します。
2. 変更するプロファイルを選択します。
3. 脅威シグネチャを除外したいアンチスパイウェア プロファイルを **Add (**追加**)** するか、既存のものを変更し、**DNS Signatures (DNS** シグネチャ**) > Exceptions (**例外**)** を選択します。
4. 名前あるいは FQDN を入力し、除外する DNS シグネチャを検索します。
5. 適用から除外するDNSシグネチャの**[DNS Threat (**脅威**) ID]**を選択します。



6. **OK** をクリックし、新しい、あるいは変更したアンチスパイウェア プロファイルを保存します。

テスト ドメイン

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced DNSセキュリティ ライセンス（拡張機能サポート用）またはDNSセキュリティ ライセンス ❑ Advanced Threat PreventionまたはThreat Preventionライセンス

Palo Alto Networksでは、DNSカテゴリーに基づいてポリシー設定を検証するために、以下のDNSセキュリティ テスト ドメインを提供しています。

STEP 1 | 次のテスト　ドメインにアクセスして、特定の脅威タイプのポリシー　アクションが実施されていることを確認します。

DNS セキュリティ

- C2—test-c2.testpanw.com
- DNS Tunneling—test-dnstun.testpanw.com
- C2—test-c2.testpanw.com
- ダイナミックDNS*—test-ddns.testpanw.com
- マルウェア—test-malware.testpanw.com
- 登録されたばかりのドメイン*—test-nrd.testpanw.com
- フィッシング*—test-phishing.testpanw.com
- グレイウェア*—test-grayware.testpanw.com
- パーク*—test-parked.testpanw.com
- プロキシ回避およびアノニマイザ*—test-proxy.testpanw.com
- 高速フラックス*—test-fastflux.testpanw.com
- 悪意のあるNRD*—test-malicious-nrd.testpanw.com
- NXNS攻撃*—test-nxns.testpanw.com
- ダングリング*—test-dangling-domain.testpanw.com
- DNSの再バインド*—test-dns-rebinding.testpanw.com
- DNS侵入*—test-dns-infiltration.testpanw.com
- ワイルドカードの悪用*—test-wildcard-abuse.testpanw.com
- 戦略的に古い*—test-strategically-aged.testpanw.com
- 侵害されたDNS*—test-compromised-dns.testpanw.com
- 広告トラッキング*—test-adtracking.testpanw.com
- CNAMEクローキング*—test-cname-cloaking.testpanw.com
- ランサムウェア*—test-ransomware.testpanw.com
- 蓄積*—test-stockpile-domain.testpanw.com
- サイバースクワッティング*—test-squatting.testpanw.com
- サブドメイン レピュテーション*—test-subdomain-reputation.testpanw.com

*印のテスト ドメインは*PAN-OS 9.1*ではサポートされていません。

高度**DNS**セキュリティ

次のテスト ドメインにアクセスして、特定の脅威タイプのポリシー アクションが実施されていることを確認します。

- **DNS**設定ミスドメイン(クレーム可能): http://test-dnsmisconfig-claimable-nx.testpanw.com

ドメインにアクセスする前に、testpanw.comのDNSサーバー ゾーン ファイルに以下のテスト ドメイン テスト ケースを追加する必要があります。これらのテスト ケースは、Advanced DNSセキュリティ シグネチャと照合され、適切なログが生成されます。特定の脅威タイプのポリシー アクションが実施されていることを確認します。

表 **1 : DNS**の設定ミス ドメイン**(**ゾーン ダングリング**)**のテスト ケース

ホスト	レコード タイプ	レコード データ
*.test-dnsmisconfig-zone-dangling.testpanw.com	A	1.2.3.4

表 **2 :** ドメイン ハイジャックのテスト ケース

ホスト	レコード タイプ	レコード データ
test-ipv4.hijacking.testpanw.com	A	1.2.3.5
*.test-ipv4-wildcard.hijacking.testpanw.com	A	1.2.3.6
test-ipv6.hijacking.testpanw.com	AAAA	2607:f8b0:4005:80d::2005
test-cname-rrname.hijacking.testpanw.com	CNAME	1.test-cname-wc.hijacking.testpanw.com
test-cname-rrname-wc.hijacking.testpanw.com	CNAME	1.test-cname-wildcard-1.hijacking.testpanw.com
*.test-cname-rrname-sub-wc.hijacking.testpanw.com	CNAME	2.test-cname-wc.hijacking.testpanw.com
test-ns-rrname.hijacking.testpanw.com	NS	test-ns.hijacking.testpanw.com
test-ns-rrname-rdata-wc.hijacking.testpanw.com	NS	1.test-ns-wc.hijacking.testpanw.com
1.test-ns-rrname-sub-wc.hijacking.testpanw.com	NS	test-ns.hijacking.testpanw.com
test-rrname-wc.hijacking.testpanw.com	NS	test-ns-2.hijacking.testpanw.com

ホスト	レコード タイプ	レコード データ

*NS*レコードの場合は、次のオプションを使用する必要があります。***dig +trace NS***

STEP 2 | アクティビティを監視して、DNSクエリ要求がDNSセキュリティによって処理されたことを確認します。

DNSセキュリティ クラウド サービスへの接続テスト

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced DNSセキュリティ ライセンス（拡張機能サポート用）またはDNSセキュリティ ライセンス ❑ Advanced Threat PreventionまたはThreat Preventionライセンス

DNS セキュリティ

DNSセキュリティ サービスへのファイアウォールの接続を確認します。サービスに到達できない場合は、以下のドメインがブロックされていないことを確認してください: dns.service.paloaltonetworks.com.

STEP 1 | ファイアウォール CLI にアクセスします。

STEP 2 | 以下のCLIコマンドを使用して、DNSセキュリティ サービスにファイアウォールが接続可能か確認します。

```
show dns-proxy dns-signature info
```

以下に例を示します。

```
show dns-proxy dns-signture info Cloud URL:
 dns.service.paloaltonetworks.com:443 Telemetry URL:
 io.dns.service.paloaltonetworks.com:443 Last Result:None
 Last Server Address:None Last Server Address:None Last Server
 Address:Interval 43200 sec Request Waiting Transmission:0 Request
 Pending Response:0 Cache Size:0
```

ファイアウォールにDNSセキュリティ サービスへのアクティブな接続がある場合、応答出力にサーバーの詳細が表示されます。

STEP 3 | レイテンシー、TTL、シグネチャのカテゴリなど、指定ドメインのトランザクション詳細を取得します。

ファイアウォール上で次のCLIコマンドを実行し、ドメインの詳細情報を表示します。

```
test dns-proxy dns-signature fqdn
```

以下に例を示します。

```
test dns-proxy dns-signature fqdn www.yahoo.com DNS
 Signature Query [ www.yahoo.com ] Completed in 178 ms
 DNS Signature Response Entries:2 Domain Category GTID TTL
 ------------------------------------------------------------------------------
 *.yahoo.com Benign 0 86400 www.yahoo.com Benign 0 3600
```

高度DNSセキュリティ

Advanced DNSセキュリティ サービスへのファイアウォールの接続を確認します。サービスに到達できない場合は、以下のドメインがブロックされていないことを確認してください: adv-dns.service.paloaltonetworks.com.地域Advanced DNSセキュリティを手動で設定している場合は、特定の地域ドメインもブロック解除されていることを確認する必要がある場合があります。

Advanced DNSセキュリティ クラウド サービスへのファイアウォール接続のステータスを確認します。

接続ステータスを表示するには、ファイアウォール上で次のCLIコマンドを実行します。

```
show ctd-agent status security-client
```

以下に例を示します。

```
show ctd-agent status security-client ...Security Client ADNS(1)
 Current cloud server: qa.adv-dns.service.paloaltonetworks.com:443
 Cloud connection: connected Config:Number of gRPC connections:2,
 Number of workers:8 Debug level:2, Insecure connection: false,
 Cert valid: true, Key valid: true, CA count:306 Maximum number
 of workers:12 Maximum number of sessions a worker should process
 before reconnect:10240 Maximum number of messages per worker:0
 Skip cert verify: false Grpc Connection Status:State Ready
 (3), last err rpc error: code = Unavailable desc = unexpected
 HTTP status code received from server:502 (Bad Gateway);
 transport: received unexpected content-type "text/html" Pool
 state:Ready (2) last update:2024-01-24 11:15:00.549591469
 -0800 PST m=+1197474.129493596 last connection retry:2024-01-23
 00:03:09.093756623 -0800 PST m=+1070762.673658768 last pool
 close:2024-01-22 14:15:50.36062031 -0800 PST m=+1035523.940522446
 Security Client AdnsTelemetry(2) Current cloud server: io-qa.adv-
dns.service.paloaltonetworks.com:443 Cloud connection: connected
 Config:Number of gRPC connections:2, Number of workers:8 Debug
 level:2, Insecure connection: false, Cert valid: true, Key valid:
```

```
 true, CA count:306 Maximum number of workers:12 Maximum number of
 sessions a worker should process before reconnect:10240 Maximum
 number of messages per worker:0 Skip cert verify: false Grpc
 Connection Status:State Ready (3), last err rpc error: code
 = Internal desc = stream terminated by RST_STREAM with error
 code:PROTOCOL_ERROR Pool state:Ready (2) last update:2024-01-24
 11:25:58.340198656 -0800 PST m=+1198131.920100772 last connection
 retry:2024-01-23 00:03:36.78141425 -0800 PST m=+1070790.361316421
 last pool close:2024-01-22 14:24:26.954340157 -0800 PST m=
+1036040.534242289 ...
```

セキュリティクライアントAdnsTelemetry(2) とセキュリティ クライアント ADNS(1)のクラウド接続ステータスがアクティブな接続を示していることを確認します。

*CLI*出力は簡潔にするために短縮されています。

Advanced DNSセキュリティ クラウド サービスに接続できない場合は、Advanced DNSサーバーがブロックされていないことを確認してください: dns.service.paloaltonetworks.com.

検索タイムアウトの設定

どこで使用できますか?	何が必要ですか?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced DNSセキュリティ ライセンス（拡張機能サポート用）またはDNSセキュリティ ライセンス ❑ Advanced Threat PreventionまたはThreat Preventionライセンス

DNS セキュリティ

接続の問題により、ファイアウォールが割り当てられた時間内にシグネチャの判定を取得できない場合、後続のすべての DNS 応答を含む要求はパススルーされます。平均遅延をチェックして、要求が設定された期間内に収まることを確認できます。平均遅延が設定された期間を超える場合は、要求がタイムアウトしないように、平均遅延よりも高い値に設定を更新することを検討してください。

STEP 1 | CLI で以下のコマンドを発行して、平均遅延を表示します。

```
show dns-proxy dns-signature counters
```

デフォルトのタイムアウト値は 100 ミリ秒です。

STEP 2 | 出力を下にスクロールして、シグネチャ クエリ API 見出しの下の遅延セクションに移動し、平均遅延が定義されたタイムアウト期間内であることを確認します。この遅延は、DNS セキュリティ サービスからシグネチャの判定を取得するのに平均してかかる時間を示します。さまざまな遅延期間の追加の待機時間統計は、平均以下と分かります。

```
Signature query API: . . . [latency ] : max 1870 (ms) min 16(ms)
 avg 27(ms) 50 or less :47246 100 or less :113 200 or less :25 400
 or less :15 else :21
```

STEP 3 | 平均遅延が一貫してデフォルトのタイムアウト値を超えている場合は、要求を特定の期間内に収めるように設定を上げることができます。**Device**（デバイス）> **Content-ID** を選択し、**Realtime Signature Lookup**（リアルタイム シグネチャ ルックアップ）設定を更新します。

STEP 4 | 変更を [コミット] します。

高度DNSセキュリティ

STEP 1 | 次のデバッグCLIコマンドを使用して、高度なDNSセキュリティ要求のラウンド トリップ時間（ミリ秒単位）の記録を表示します。これらは、0ミリ秒から450ミリ秒までの遅延ブラケットに分配されます。これを使用して、NGFWの理想的な最大遅延設定を決定できます。

```
admin@PA-VM debug dataplane show ctd feature-forward stats
```

応答の出力で、`PAN_CTDF_DETECT_SERVICE_ADNS`セクションに移動します。

```
PAN_CTDF_DETECT_SERVICE_ADNS cli_timeout:1 req_total:2
 req_timed_out:0 Hold: adns rtt>=0ms:0 adns rtt>=50ms:2 adns
 rtt>=100ms:0 adns rtt>=150ms:0 adns rtt>=200ms:0 adns rtt>=250ms:0
 adns rtt>=300ms:0 adns rtt>=350ms:0 adns rtt>=400ms:0 adns
 rtt>=450ms:0
```

STEP 2 | ［Advanced DNS signature lookup timeout (Advanced DNSシグネチャ検索のタイムアウト)］の最大設定値を設定します。この値を超えると、Advanced DNSセキュリティを使用して解析を実行せずにDNS応答が通過します。定期的なコンテンツ更新を通じて配信される、または設定されたEDL（外部動的リスト）またはDNS例外の一部であるDNSシグネチャ（および関連するポリシー）は、引き続き適用されます。

1. **[Device (デバイス) > [Setup (セットアップ)] > [Content-ID (コンテンツID)]) > [Advanced DNS Security (Advanced DNSセキュリティ)]**を選択します。
2. ［Advanced DNS signature lookup timeout (Advanced DNSシグネチャ検索のタイムアウト)］の最大更新時間をミリ秒単位で指定します。デフォルトは100ミリ秒で、推奨設定です。

3. **OK** をクリックして変更を確定します。

または、次のCLIコマンドを使用して、Advanced DNSセキュリティのタイムアウト値を設定することもできます。100～15,000ミリ秒の値を100ミリ秒単位で設定できます。デフォルト値は100ミリ秒で、推奨設定です。

```
admin@PA-VM#set deviceconfig setting adns-setting max-latency
 <timeout_value_in_milliseconds>
```

以下に例を示します。

```
admin@PA-VM# set deviceconfig setting adns-setting max-latency 500
```

現在のタイムアウト設定は、次のCLIコマンドを使用して確認できます（出力の**max-latency**エントリを参照）。

```
admin@PA-VM show config pushed-template ... }
 deviceconfig { setting { dns { dns-cloud-server dns-
qa.service.paloaltonetworks.com; } adns-setting { max-latency
 100; } } } ...
```

DNSセキュリティ サブスクリプション サービスのバイパス

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced DNSセキュリティ ライセンス（拡張機能サポート用）またはDNSセキュリティ ライセンス ❑ Advanced Threat PreventionまたはThreat Preventionライセンス

DNSセキュリティ クエリは、遅延の問題やその他のネットワークの問題がある場合にバイパスできます。

誤検知が発生するケースでは、*DNS*セキュリティ クエリをバイパスするのではなく、特定の例外を作成することをお勧めします。

- クラウド管理
- PAN-OS & Panorama

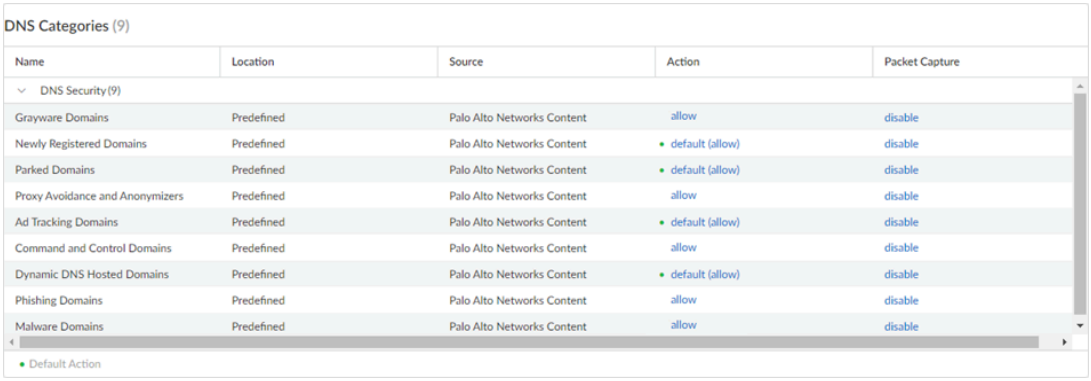
DNSセキュリティ サブスクリプション サービスのバイパス (Strata Cloud Manager)

STEP 1 | Palo Alto Networksのサポート アカウントに関連付けられた資格情報を使用し、ハブ上のStrata Cloud Managerにログインします。

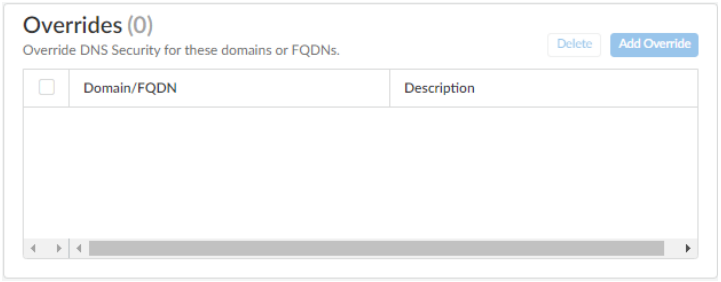
STEP 2 | **[Manage (管理)]** > **[Configuration (設定)]** > **[NGFW]Prisma Access** > **[Security Services (セキュリティ サービス)]** > **[DNS Security (DNSセキュリティ)]**に移動し、関連するDNSセキュリティ プロファイルを選択します。

STEP 3 | DNSセキュリティ クエリをバイパスするように DNSセキュリティ シグネチャ ポリシー設定を構成します。DNSカテゴリーごとに、**[Action (アクション)]**を**[allow (許可)]**に、**[Packet**

Capture (パケット キャプチャ)]を**[disabled (無効)]**に設定します。以下のDNSセキュリティ カテゴリーはDNSセキュリティ クエリをバイパスするように構成されています。



STEP 4 | **[Overrides (オーバーライド)]**セクションで、エントリが存在しないことを確認します。必要に応じて、**[Domain/FQDN (ドメイン/FQDN)]**をすべて削除します。



STEP 5 | **[OK]** をクリックしてDNSセキュリティ プロファイルを保存します。

DNSセキュリティ サブスクリプション サービスのバイパス (NGFW (Managed by PAN-OS or Panorama))

PAN-OS 10.0以降では、個別に設定可能なDNSシグネチャ ソースがサポートされており、特定のシグネチャ ソースに対してログの重大度レベルだけでなく、個別のポリシー アクションを定義することができます。そのためには、DNSセキュリティをバイパスするために、使用可能なDNSシグネチャ ソースごとにポリシーアクションとログ重大度の両方を設定する必要があります。さらに、DNSセキュリティを完全にバイパスするには、DNS例外エントリも削除する必要があります。PAN-OS 9.1では、Palo Alto Networks DNSセキュリティのポリシーアクションを許可のアクションに設定できるだけです。

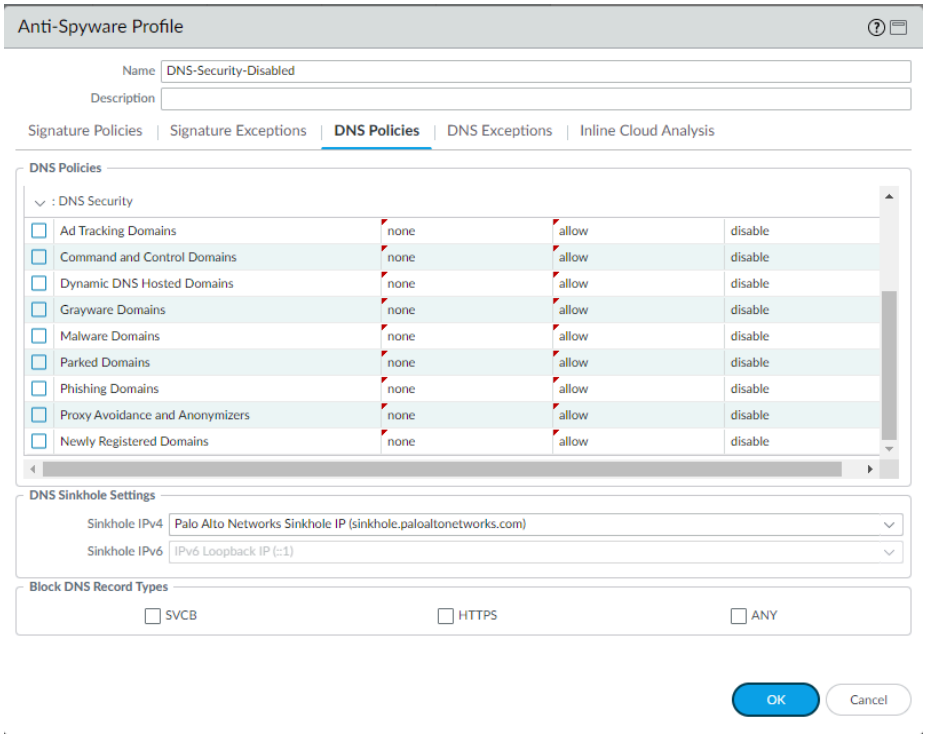
- PAN-OS 10.0 以降
- PAN-OS 9.1

DNSセキュリティ サブスクリプション サービスのバイパス (PAN-OS 10.0以降)

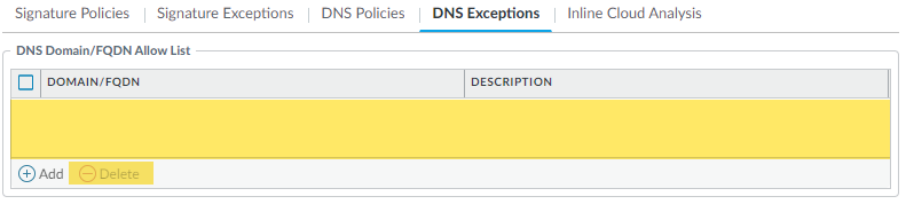
STEP 1 | NGFWにログインします。

STEP 2 | DNSセキュリティ クエリをバイパスするようにDNSセキュリティ シグネチャ ポリシー設定を構成します。

1. **Objects (オブジェクト) > > Security Profiles (セキュリティ プロファイル) > > Anti-Spyware (アンチスパイウェア)** を選択します。
2. アクティブなDNSセキュリティ ポリシー設定を含むプロファイルを選択します。
3. **DNS Policies (DNS ポリシー)** タブを選択します。
4. 各DNSカテゴリーについて、ログの重大度を**none**に、ポリシー アクションを **allow**に、パケット キャプチャを**disabled**に設定します。以下のDNSセキュリティ カテゴリーはDNSセキュリティ クエリをバイパスするように構成されています。



STEP 3 | **DNS**例外を選択し、すべての**DNS**ドメイン/**FQDN**許可リストエントリを削除します。



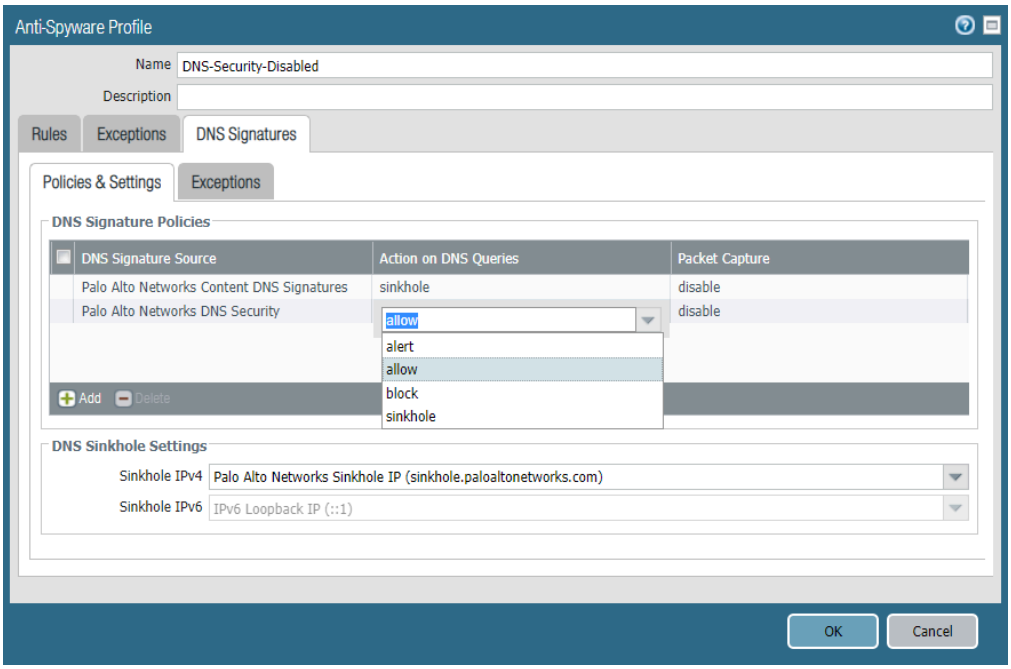
STEP 4 | **OK** をクリックし、アンチスパイウェア プロファイルを保存します。

DNSセキュリティ サブスクリプション サービスのバイパス（PAN-OS 9.1）

STEP 1 | NGFWにログインします。

STEP 2 | DNSセキュリティ シグネチャ ポリシーの設定で、DNSセキュリティ ルックアップをバイパスするように設定します。

1. **Objects (オブジェクト) > > Security Profiles (セキュリティ プロファイル) > > Anti-Spyware (アンチスパイウェア)** を選択します。
2. アクティブなDNSセキュリティ ポリシー設定を含むプロファイルを選択します。
3. **[DNS Signatures (DNSシグネチャ)]** タブを選択します。
4. **[Policies & Settings (ポリシーと設定)]**で、**[Palo Alto Networks DNS Security (Palo Alto NetworksのDNSセキュリティ)]**のポリシーアクションを**[allow (許可)]**のアクションに設定します。



STEP 3 | **OK** をクリックし、アンチスパイウェア プロファイルを保存します。

DNSセキュリティ サブスクリプション サービスの監視

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced DNSセキュリティ ライセンス（拡張機能サポート用）またはDNSセキュリティ ライセンス ❑ Advanced Threat PreventionまたはThreat Preventionライセンス

Palo Alto Networksは、DNSセキュリティ サブスクリプション サービスおよび関連するトラフィック データに依存するさまざまな製品のインテリジェンス検索に対応するため、DNSセキュリティおよびAdvanced DNSセキュリティ アクティビティを監視するいくつかのオプションを提供しています。製品プラットフォームによっては、ネットワーク アクティビティのコンテキストを含むDNSリクエストの統計と使用状況の傾向、特定のユーザーからの特定のDNS要求の詳細をログ データの形式で提供する、高レベルのダッシュボードにアクセスできます。

また、DNSセキュリティ サブスクリプション サービスが他のPalo Alto Networksアプリケーションやセキュリティ サービスと統合され、組織を脅威から保護する方法や、Strata Cloud Managerコマンドセンターからデプロイメントの運用状態全体を大まかに把握することもできます。コマンド センターはNetSecのホームページとして機能し、ネットワークの健全性、セキュリティ、および効率性の包括的なサマリーを、複数のデータ ファセットを備えたインタラクティブなビジュアル ダッシュボードで提供します。これにより、一目で簡単に評価できます。

DNSセキュリティ サブスクリプション サービスの運用に関するより具体的な詳細については、ダッシュボードでネットワークDNSクエリ データを確認できるほか、さまざまなDNSトレンドをドリルダウンできます。各ダッシュボード カードでは、DNS要求と応答の処理方法を独自のビューで表示し、グラフィカルなレポート形式で分類できます。これにより、組織のDNS使用状況の統計を一目で詳細に把握できます。またAdvanced DNSセキュリティ サービスによって検出された、誤って設定されたドメインや乗っ取られたドメインの一覧も表示されるため、DNS設定エラーを修正および是正することができます。正しく構成されていないドメインは、**[DNS Zone Misconfigurations (DNS**ゾーンの設定ミス**)]**リストに追加されたパブリック向けの親ドメイン エントリに基づいています。

DNS要求が処理されたときに自動的に生成されるログを表示することもできます。これらのイベント ファイルにはタイムスタンプが付けられ、DNSカテゴリー ログ設定に基づいて監査証跡が付与されます。DNSログ エントリには、関連するドメインによって引き起こされたDNS脅威の

性質や、脅威が検出されたときの処理など、DNS要求に関するさまざまな詳細を含めることができます。

Palo Alto Networksは、プラットフォームに基づいてDNSセキュリティ アクティビティを監視するためのいくつかの方法を提供しています。

- Strata Cloud Managerコマンド センター
- DNSセキュリティ ダッシュボードの表示
- ネットワークを通過したDNSクエリのDNSセキュリティ ログを表示する

DNSセキュリティ ダッシュボードの表示

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced DNSセキュリティ ライセンス（拡張機能サポート用）またはDNSセキュリティ ライセンス ❑ Advanced Threat PreventionまたはThreat Preventionライセンス

DNSセキュリティ ダッシュボードでは、組織のDNS使用状況の高速かつ視覚的な評価レポートに、Advanced DNSセキュリティおよびDNSセキュリティ サブスクリプション サービスで生成された統計データが表示されます。ネットワークで検出されたさまざまなDNSトレンドを表示し、ドリルダウンできます。各ダッシュボード カードでは、DNS要求の処理方法と分類方法を独自のビューで確認できます。ダッシュボード カードを選択すると、ダッシュボードのコンテキストを変更したり、特定の傾向、ドメイン、統計に関する詳細情報を表示したりできます。

DNSセキュリティ ダッシュボードは、Prisma AccessとAIOps for NGFWで利用できます。DNSセキュリティ ダッシュボード カードとやり取りしてダッシュボードのコンテキストを変更したり、特定の傾向、ドメイン、統計に関する詳細情報を表示したりできます。また、関連するデータ ポイント間で、現在の傾向や履歴データを表示するようにフォーマットをカスタマイズすることもできます。

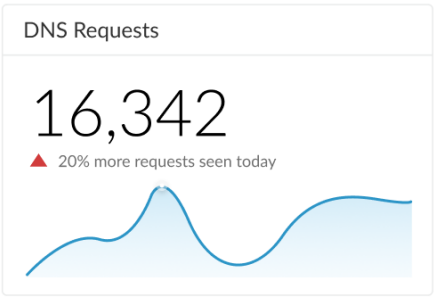
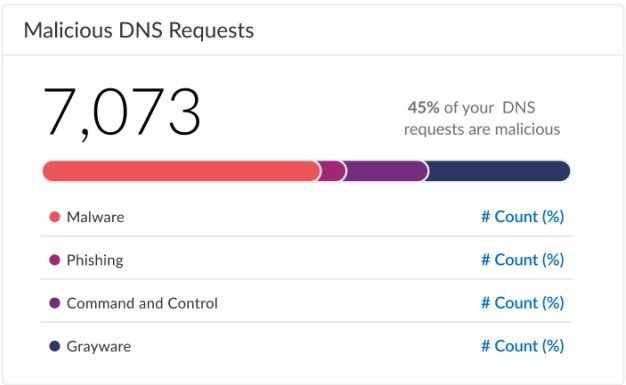
- Strata Cloud Manager
- AIOps for NGFW Free

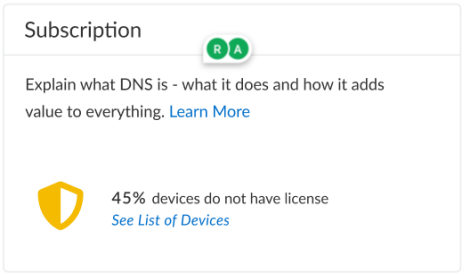
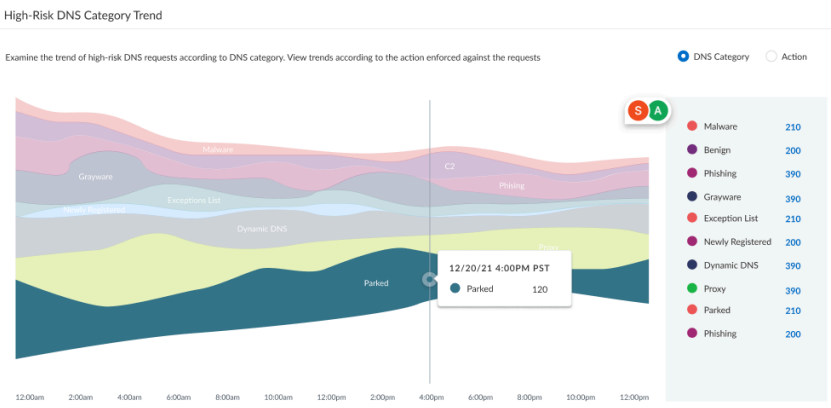
DNSセキュリティ ダッシュボード カード

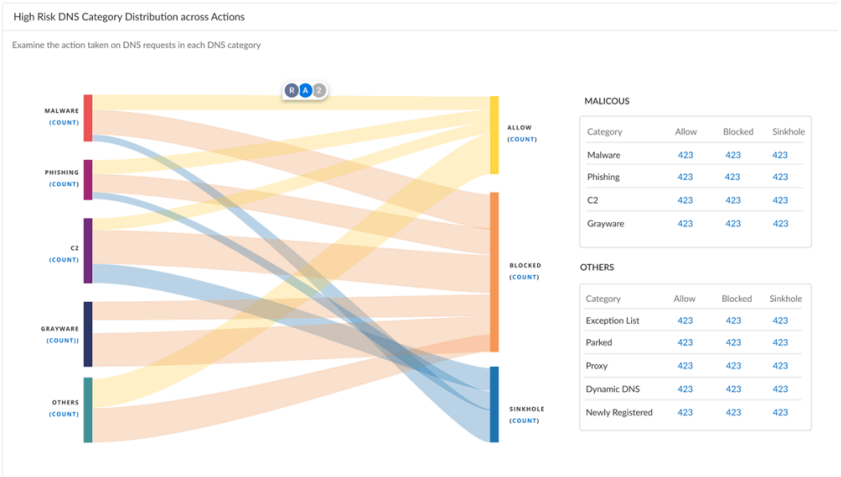
どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced DNSセキュリティ ライセンス（拡張機能サポート用）またはDNSセキュリティ ライセンス ❑ Advanced Threat PreventionまたはThreat Preventionライセンス

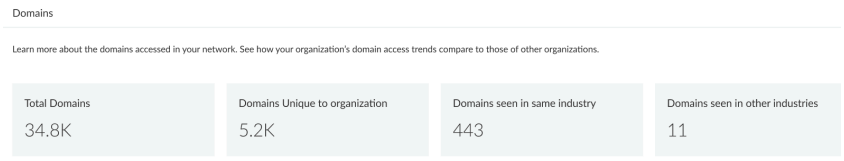
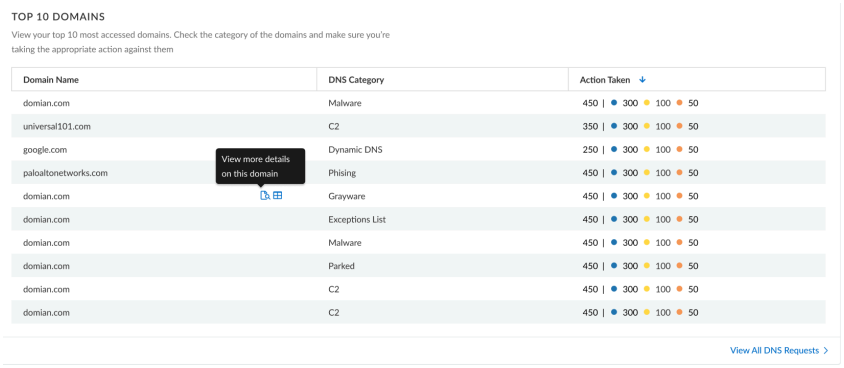
DNSセキュリティ ダッシュボードに入力するカードはインタラクティブで、コンテンツの表示方法に関係するため、追加の詳細を表示したり、特定の要求、イベント、ドメインのリストにピボットしたりできます。

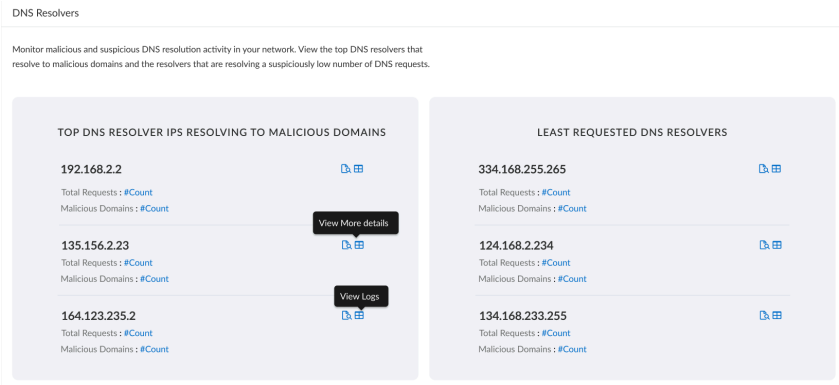
DNSセキュリティ ダッシュボード カードの概要を次に示します。

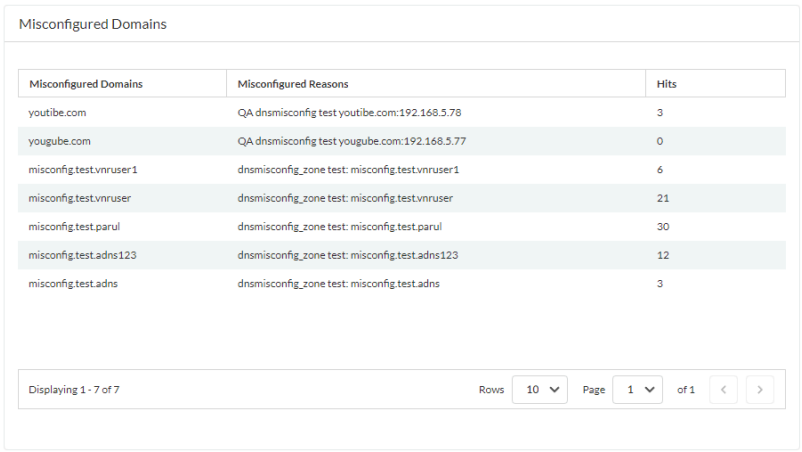
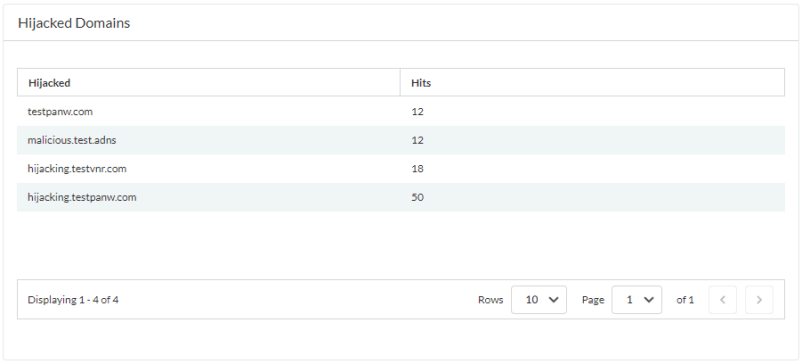
カード名	詳説
DNS リクエスト	DNSセキュリティによって処理されたDNS要求の総数が表示されます。  • 折れ線グラフは、ユーザーが定義した時間範囲に基づくDNS要求の数を示します。カスタム時間範囲を指定すると、それに応じて折れ線グラフが更新されます。 • DNSカテゴリーおよびアクションフィルタは、カードの内容を変更することはありません。
悪意のあるDNSリクエスト数	現在利用可能なタイプに基づいて分類されたDNS要求のうち、悪意のあるものと考えられるものを積み重ねた棒グラフを表示します。カテゴリー変数の内訳を以下に示す一方で、合計数は左上に示しています。  • 折れ線グラフは、ユーザーが定義した時間範囲に基づくDNS要求の数を示します。カスタム時間範囲を指定すると、それに応じて折れ線グラフが更新されます。

カード名	詳説
	• DNSカテゴリーおよびアクションフィルタは、カードの内容を変更することはありません。
サブスクリプション	DNSセキュリティ サブスクリプションが有効なネットワーク内のデバイスの数が表示されます。DNSセキュリティが搭載されていない、または契約が経過するデバイスの割合も、完全なリストへのリンクとともに表示されます。  • **[See a List of Devices (**デバイスのリストを見る**)]**を選択すると、すべてのリストを表示できます。 • このカードは、現在のサブスクリプション ステータスのスナップショットを示します。フィルタ オプションは影響しません。
高リスクDNSカテゴリの傾向	DNSカテゴリーに基づくDNS要求の内訳、または観測可能な時間範囲のDNS要求に適用されるアクションを示すトレンド チャートを表示します。  • DNSカテゴリーまたはアクション トレンド チャートのいずれかをラジオ ボタンを使用して選択します。

カード名	詳説
	• データ型を表すストリームグラフ上のセグメントにカーソルを合わせると、DNS要求の数または実行されたアクションの種類を示すポップアップが分離されて開きます。 • カスタム時間範囲を指定すると、それに応じてトレンドチャートが更新されます。 • DNSカテゴリーとアクションフィルタは、カード内の選択した変数を強調表示しますが、グラフから削除はしません。
アクション間のDNSカテゴリーの配布	ハイリスクDNSカテゴリーに対して行われたアクションの分布を可視化したフロー図を表示します。セカンダリ テーブルは、優先順位の低いDNSカテゴリーに対して実行されるアクションを示します。 • 特定のフローにカーソルを合わせると、指定した種類のアクションの数を示すポップアップが開きます。 カスタム時間範囲を指定すると、それに応じてフロー図が更新されます。 • DNSカテゴリーおよびアクションフィルタは、カードの内容を変更することはありません。  • トップ ドメイン リストは、ダッシュボードの上部で適用されるフィルタ設定に基づいて生成されます。ページ設定全体に影響するウィジェットは、表示するドメインも決定します。 • バーにカーソルを合わせると、使用状況の統計が表示されます。 • ドメインをクリックするとDNS解析の詳細が表示されます。

カード名	詳説
ドメイン	選択したDNSカテゴリーに基づいて、ネットワーク内、業界内、他業界内で見られるドメイン数と合計数を表示します。組織のDNS使用状況を業界内の他の組織と比較したり、ネットワーク内でのみ見つかったドメインリクエスト要求のリストなど、グローバルに収集されたデータと比較したりできます。  • このカードに記載されているドメインは、DNSカテゴリーやアクション フィルタに関係なく、すべてのDNSカテゴリーが含まれています。時間範囲だけがカードの内容を更新します。
トップ10ドメイン	DNSカテゴリーと実行されたアクションとともに、ネットワークから最もよく要求されるドメインの上位10のリストを提供します。該当するアイコンをクリックすると、ドメインの詳細と関連するログを表示できます。アクセスされたドメインの完全なリストを表示するには、**[View All DNS Request (**すべての**DNS**要求を表示**)]**を選択します。 

カード名	詳説
	• このカードに記載されているドメインは、DNSカテゴリーやアクション フィルタに関係なく、すべてのDNSカテゴリーが含まれています。時間範囲だけがカードの内容を更新します。 • ドメインをクリックするとDNS解析の詳細が表示されます。
DNSリゾルバー	ネットワーク内で最も解決された悪意のあるドメインと最も解決されなかったドメインを示す2つのリストを提供します。  • DNSリゾルバーをクリックすると、DNS解析の詳細が表示されます。
ドメインの設定ミス(Advanced DNSセキュリティ)	ユーザーが指定した公開親ドメインに関連付けられた解決不能ドメインのリストを提供します。エントリごとに、設定ミスの理由と、送信元IPに基づくトラフィック ヒット数があります。

カード名	詳説
	
ハイジャックされたドメイン（Advanced DNSセキュリティ）	ハイジャックされたドメインのリストを、Advanced DNSセキュリティによって決定されたとおりに提供します。エントリごとに、送信元IPに基づいた分類理由とトラフィック ヒット数があります。 

DNSセキュリティ ダッシュボードの表示 (Strata Cloud Manager)

STEP 1 | Palo Alto Networksのサポート アカウントに関連付けられた資格情報を使用し、ハブ上のStrata Cloud Managerにログインします。

STEP 2 | **[Dashboard (ダッシュボード)]** > **[More Dashboards (その他のダッシュボード)]** > **[DNS Security (DNSセキュリティ)]**を選択し、DNSセキュリティ ダッシュボードを開きます。

STEP 3 | ダッシュボードから、利用可能なドロップ ダウンを使用してフィルター オプションを設定します。

1. ［Filter by time range (時間範囲でフィルタ)］:［**Last hour (過去1時間)**］、［**Last 24 hours (過去24時間)]**、［**Last 7 days (過去7日間)]**、または**[Last 30 days (過去30日間)**］から選択して、特定の期間のデータを表示します。
2. [Filter by DNS category （DNSカテゴリーでフィルタ)]: **[Select All (すべて選択)]**、**[Malware (マルウェア)]**、**[Command and Control (コマンドとコントロール)]**、**[Phishing (フィッシング)]**、**[Grayware (グレーウェア)]**、**[Exceptions List (例外リスト)**］、**[Newly Registered (新規登録)**］、**[Dynamic DNS (ダイナミックDNS)]**、**[Proxy (プロキシ)**］、**[Parked (パーク)**］、**[Benign (良性)**］、**[Ad Track (広告トラック)**］から選択し、DNSタイプに基づくデータ セットをフィルタします。

   例外リスト カテゴリーは、*PAN-DB*と*Alexa*からのメトリックに基づいて明示的に許可されるドメインのリストで、*Palo Alto Networks*が管理しています。これらの許可リスト ドメインは頻繁にアクセスされ、悪意のあるコンテンツがないことが分かっています。
3. ［Filter by DNS action (DNSアクションでフィルタ)］: **[Allow (許可)**］、［**Block （ブロック）**］、および**[Sinkhole (シンクホール)**］から選択し、DNSセキュリティ プロファイルのアクション設定からDNSクエリに対して実行されるアクションに基づいてフィルタリングします。

STEP 4 | オプションで、アクティビティ レポートのダウンロード、共有、スケジュール設定もできます。

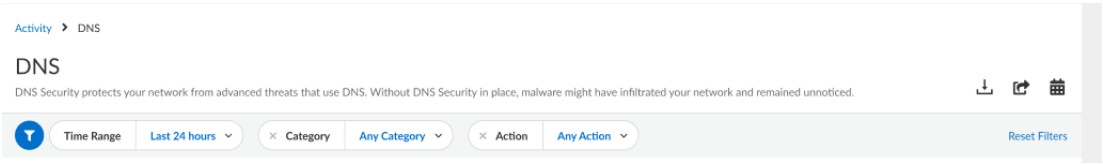
STEP 5 | ダッシュボード カードが提供するデータから、再コンテキスト化、インタラクション、ピボットを行うことができます。DNSセキュリティ ダッシュボードの各カードの概要については、「DNSセキュリティ ダッシュボード カード」を参照してください。

DNSセキュリティ ダッシュボードの表示 (AIOps for NGFW Free)

STEP 1 | Palo Alto Networksのサポート アカウントに関連付けられた資格情報を使用し、ハブ上のAIOps for NGFW Freeアプリケーションにログインします。

STEP 2 | **[Dashboard (ダッシュボード)]** > **[More Dashboards (その他のダッシュボード)]** > **[DNS Security (DNSセキュリティ)]**を選択し、DNSセキュリティ ダッシュボードを開きます。

STEP 3 | ダッシュボードから、利用可能なドロップ ダウンを使用してフィルター オプションを設定します。



1. ［Filter by time range (時間範囲でフィルタ)］:［**Last hour (過去1時間)**］、［**Last 24 hours (過去24時間)]**、［**Last 7 days (過去7日間)]**、または**[Last 30 days (過去30日間)**］から選択して、特定の期間のデータを表示します。
2. [Filter by DNS category (DNSカテゴリによるフィルタ)]: **[C2 (DGA, Tunneling, other C2 (C2（DGA**、トンネリング、その他**C2)]**、**[Malware (マルウェア)]**、**[Newly Registered Domain (新規登録ドメイン)]**、**[Phishing (フィッシング)]**、**[Dynamic DNS (ダイナミック**DNS)]、**[Allow List (許可リスト)]**、**[Benigh (良性)**］、**[Grayware (グレーウェア)]**、**[Parked (パーク)]**、**[Proxy (プロキシ)]**］、［**Any Category (任意のカテゴリー)]**から選択し、DNSタイプに基づいたデータ セットをフィルタします。

   許可リスト カテゴリーは、*PAN-DB*と*Alexa*からのメトリックに基づいて明示的に許可されるドメインのリストで、*Palo Alto Networks*が管理しています。これらの許可リスト ドメインは頻繁にアクセスされ、悪意のあるコンテンツがないことが分かっています。
3. ［Filter by DNS action (DNSアクションでフィルタ)］: **[Allow (許可)**］、［**Block** （ブロック）］、および**[Sinkhole (シンクホール)**］から選択し、DNSセキュリティ プロファイルのアクション設定からDNSクエリに対して実行されるアクションに基づいてフィルタリングします。

STEP 4 | オプションで、アクティビティレポートのダウンロード、共有、スケジュール設定もできます。

STEP 5 | ダッシュボード カードが提供するデータから、再コンテキスト化、インタラクション、ピボットを行うことができます。DNSセキュリティ ダッシュボードの各カードの概要については、「DNSセキュリティ ダッシュボード カード」を参照してください。

DNSセキュリティ ログの表示

どこで使用できますか?	何が必要ですか?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ Advanced DNSセキュリティ ライセンス（拡張機能サポート用）またはDNSセキュリティ ライセンス ❑ Advanced Threat PreventionまたはThreat Preventionライセンス

DNSセキュリティが適格なイベントに遭遇したときに自動的に生成されるDNSセキュリティ ログを参照、検索、表示できます。通常、ログの重大度レベルがnoneに明示的に設定されていない限り、DNSセキュリティが分析するすべてのドメイン カテゴリーが含まれます。ログ エントリには、脅威のレベルや、該当する場合は脅威の性質など、イベントに関するさまざまな詳細が提供されます。

DNSセキュリティ ログはファイアウォールから直接アクセスすることも、Strata Logging Serviceベースのログ ビューアー（AIOps for NGFW Free、Cloud Management、Strata Logging Serviceなど）を通してアクセスすることもできます。ファイアウォールでは、ユーザーがDNSクエリを実行したときに生成される悪意のある脅威のログ エントリにアクセスできますが、無害なDNS要求は記録されません。DNSセキュリティ データもStrata Logging Serviceにログ転送(脅威ログとして)およびDNSセキュリティ テレメトリ (DNSセキュリティ ログとして) を介して転送され、さまざまなアクティビティ ログ ビューアー アプリケーションによって参照されます。DNSセキュリティ テレメトリは最小限のオーバーヘッドで動作し、Strata Logging Serviceに送信されるデータの量を制限します。その結果、DNSクエリのサブセットのみが重大度レベル、脅威の種類、またはカテゴリに関係なく、DNS セキュリティ ログ エントリとしてStrata Logging Serviceに転送されます。ログ転送を使用してStrata Logging Serviceに転送される悪意のあるDNS要求の脅威ログはすべての機能が利用可能です。そのため、Palo Alto Networksは、悪意のあるDNSリクエスト要求のログをDNSセキュリティ ログではなく脅威ログとして表示することを推奨しています。

- Strata Cloud Manager
- PAN-OS & Panorama
- AIOps for NGFW Free
- Strata Logging Service

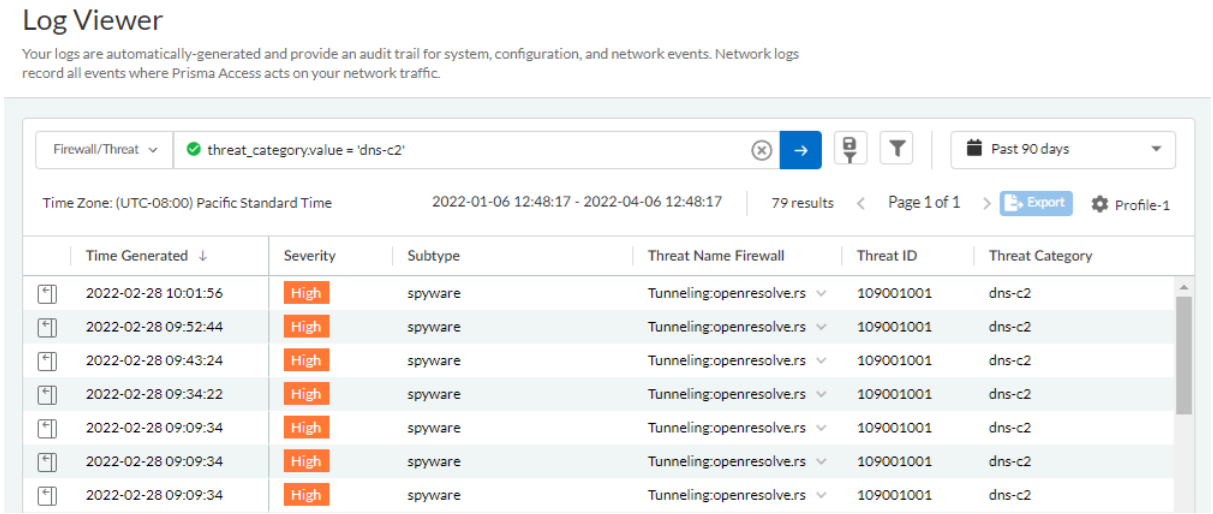
DNSセキュリティ ログの表示 (Strata Cloud Manager)

*DNS*セキュリティで解析された問題のない*DNS*クエリは、ログ ビューアーに表示されません。*Strata Logging Service*アプリにログインし、問題のない*DNS*ログ エントリにアクセスします。

STEP 1 | Palo Alto Networksのサポート アカウントに関連付けられた資格情報を使用し、ハブ上のStrata Cloud Managerにログインします。

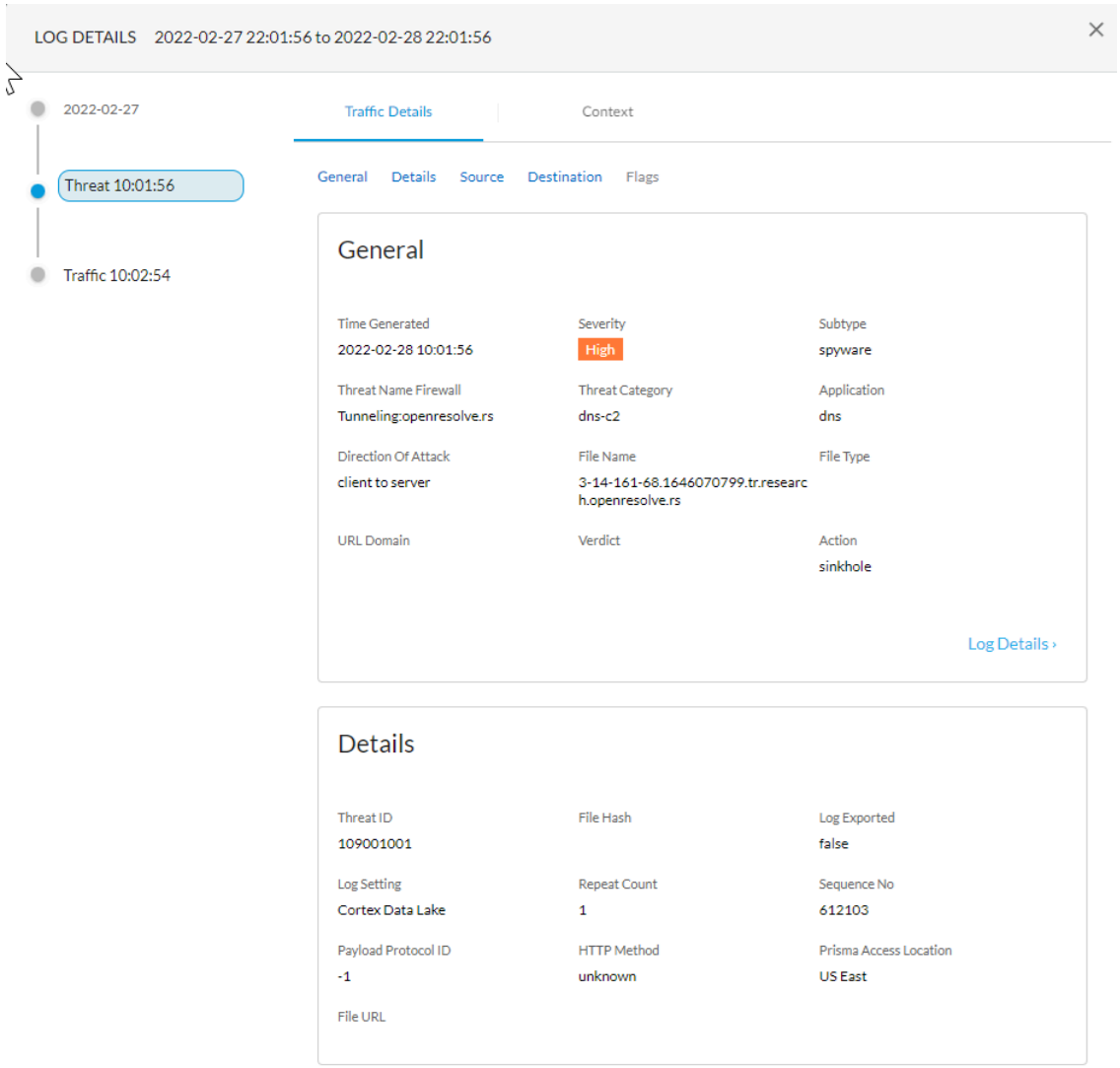
STEP 2 | DNSセキュリティを使用して処理されたDNSクエリを検索します。

1. **[Incidents and Alerts (インシデントとアラート)]** > **[Log Viewer (ログ ビューアー)]**を選択します。
2. 脅威フィルタを使用して検索を制限し、DNSカテゴリーに基づいてログ クエリを送信します。たとえば、`threat_category.value = 'dns-c2'`と指定すると、C2ドメインと判定されたログが表示されます。他のDNSタイプを検索するには、c2をサポートされている別のDNSカテゴリー（ddns、parking、malwareなど）に置き換えます。必要に応じて、追加のクエリ パラメータ (重大度レベルやサブタイプなど) や日付範囲など、検索条件を調整します。



3. ログ エントリを選択して、検出されたDNS脅威の詳細を表示します。

4. 脅威カテゴリー は、詳細ログ ビューの**[General (全般)]**ペインに表示されます。脅威に関するその他の関連詳細は、対応するウィンドウに表示されます。



5. 蓄積されたドメインや、トンネリングベースのAPT (advanced persistent threat (APT攻撃 -APT))を含むDNSトンネリング ドメインについては、攻撃に使用されたさまざまなツールや、ドメインに関連付けられた攻撃キャンペーンを表示できます。これは、特定のドメインのログ エントリの脅威ID/名前フィールドに反映されます。属性付きDNSドメインの脅威ID/名前には、次の形式を使用します。この例では、DNSトンネル ドメインの場合です。トンネリング`:<tool_name>`、`<tool_name>`、`<tool_name>`、`...:<domain_name>`ここで、`tool_name`は、DNSクエリと応答にデータを埋め込むために使用されるDNSトンネリング ツールを指しますが、サイバー脅威キャンペーン名もコンマ区切りのリストで示されます。これらのキャンペーンは業界で認められたインシデントであり、同じ命名規則を使用している可能性がありますが、Palo Alto Networksによって特定および命名され、Unit 42 Threat Researchブログで説明されているものかもしれません。このような

キャンペーン（この場合、DNSトンネリング技術を活用したキャンペーン）のブログは、こちらでご覧いただけます。追跡とスキャンにDNSトンネリングを活用します。

関連するツールとキャンペーンの属性は、最初の検出が完了してから、ログ、*Palo Alto Networks ThreatVault*、*Test-A-Site*に表示されるまで、しばらく時間がかかる場合があります。属性コンポーネントが終了し、検証されると、完全な*DNS*トンネリング ツールとキャンペーンの詳細が、脅威 *ID*/名前とキャンペーン フィールドに期待どおりに表示されます。

DNSセキュリティ ログの表示 (NGFW (Managed by PAN-OS or Panorama))

STEP 1 | PAN-OS Web インターフェイスにログインします。

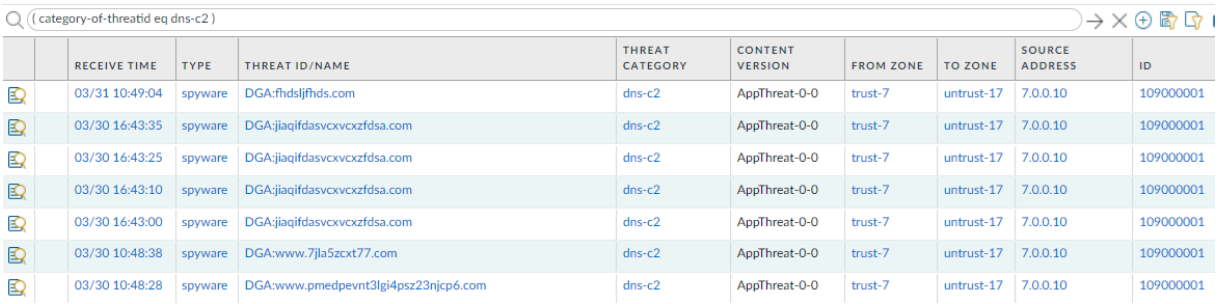
STEP 2 | DNSセキュリティを使用して処理されたクエリのファイアウォール上のアクティビティを検索します。

1. **[Monitor (監視)]** > **[Logs (ログ)]** > **[Threat (脅威)]**を選択し、DNSカテゴリーに基づいてフィルタリングします。

   次の例を考えてみてください。

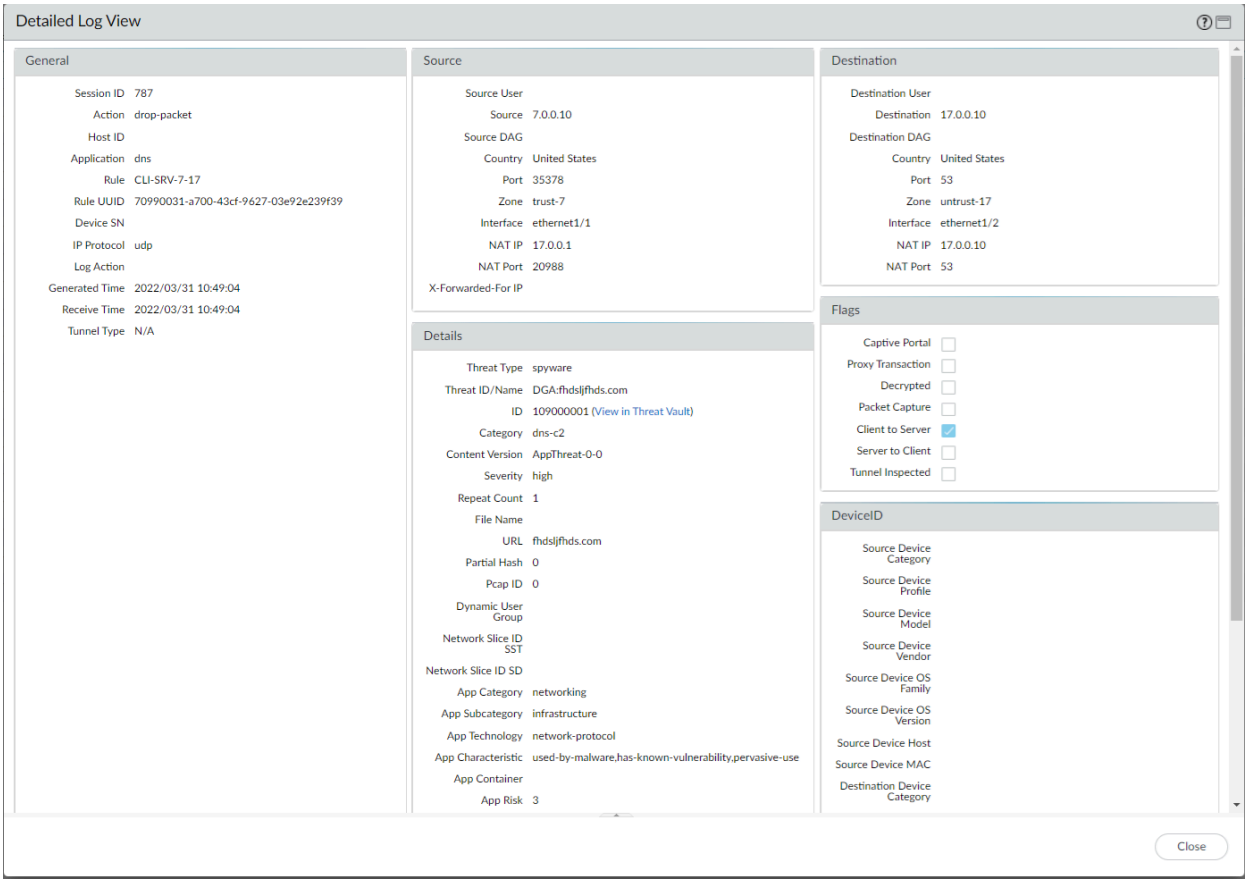
   - `(category-of-threatid eq dns-c2)`でDNSセキュリティによってC2ドメインと判定されたログを閲覧できます。
   - （`category-of-threatid eq adns-hijacking`）。変数`adns-hijacking`は、Advanced DNSセキュリティによって悪意あるDNSハイジャック試行として分類されたDNSクエリを示します。

   他のDNSタイプを検索するには、c2をサポートされている別のDNSカテゴリー（ddns、parking、malwareなど）に置き換えます。



	RECEIVE TIME	TYPE	THREAT ID/NAME	THREAT CATEGORY	CONTENT VERSION	FROM ZONE	TO ZONE	SOURCE ADDRESS	ID
	03/31 10:49:04	spyware	DGA:fhdsljfhds.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:35	spyware	DGA:jiaqifdasvcxvcxzfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:25	spyware	DGA:jiaqifdasvcxvcxzfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:10	spyware	DGA:jiaqifdasvcxvcxzfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:00	spyware	DGA:jiaqifdasvcxvcxzfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 10:48:38	spyware	DGA:www.7jla5zcxt77.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 10:48:28	spyware	DGA:www.pmedpevnt3lgi4psz23njcp6.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001

2. ログ エントリを選択して、検出されたDNS脅威の詳細を表示します。
3. 脅威カテゴリー は、詳細ログ ビューの**[Details (詳細)]**ペインに表示されます。脅威に関するその他の関連詳細は、対応するウィンドウに表示されます。



4. 蓄積されたドメインや、トンネリングベースのAPT (advanced persistent threat (APT攻撃 -APT)) を含むDNSトンネリング ドメインについては、攻撃に使用されたさまざまなツールや、ドメインに関連付けられた攻撃キャンペーンを表示できます。これは、特定のドメインのログ エントリの脅威ID/名前フィールドに反映されます。属性付きDNSドメインの脅威ID/名前には、次の形式を使用します。この例では、DNSトンネル ドメインの場合です。トンネリング:`<tool_name>`、`<tool_name>`、`<tool_name>`、`...:<domain_name>`ここで、`tool_name`は 、DNSクエリと応答にデータを埋め込むために使用されるDNSトンネリング ツールを指しますが、サイバー脅威キャンペーン名もコンマ区切りのリストで示されます。これらのキャンペーンは業界で認められたインシデントであり、同じ命名規則を使用している可能性がありますが、Palo Alto Networksによって特定および命名され、Unit 42 Threat Researchブログで説明されているものかもしれません。このようなキャンペーン（この場合、DNSトンネリング技術を活用したキャンペーン）のブログは、こちらでご覧いただけます。追跡とスキャンにDNSトンネリングを活用します。ま

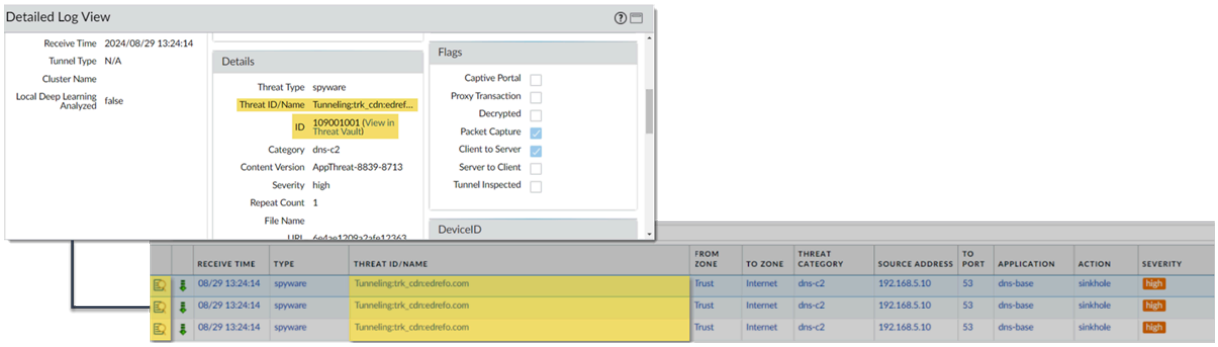
たは、Palo Alto NetworksのThreatVaultおよびURLフィルタリング テストAサイトから属性情報を表示することもできます。

関連するツールとキャンペーンの属性は、最初の検出が完了してから、ログ、*Palo Alto Networks ThreatVault*、*Test-A-Site*に表示されるまで、しばらく時間がかかる場合があります。属性コンポーネントが終了し、検証されると、完全な*DNS*トンネリング ツールとキャンペーンの詳細が、脅威 *ID*/名前とキャンペーン フィールドに期待どおりに表示されます。

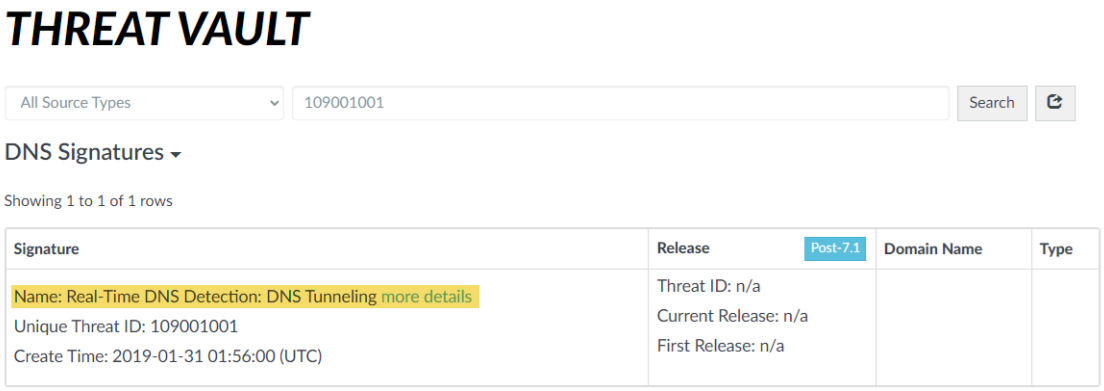
次の例を考えてみてください。

- **DNS**トンネリング ドメインの**APT**属性

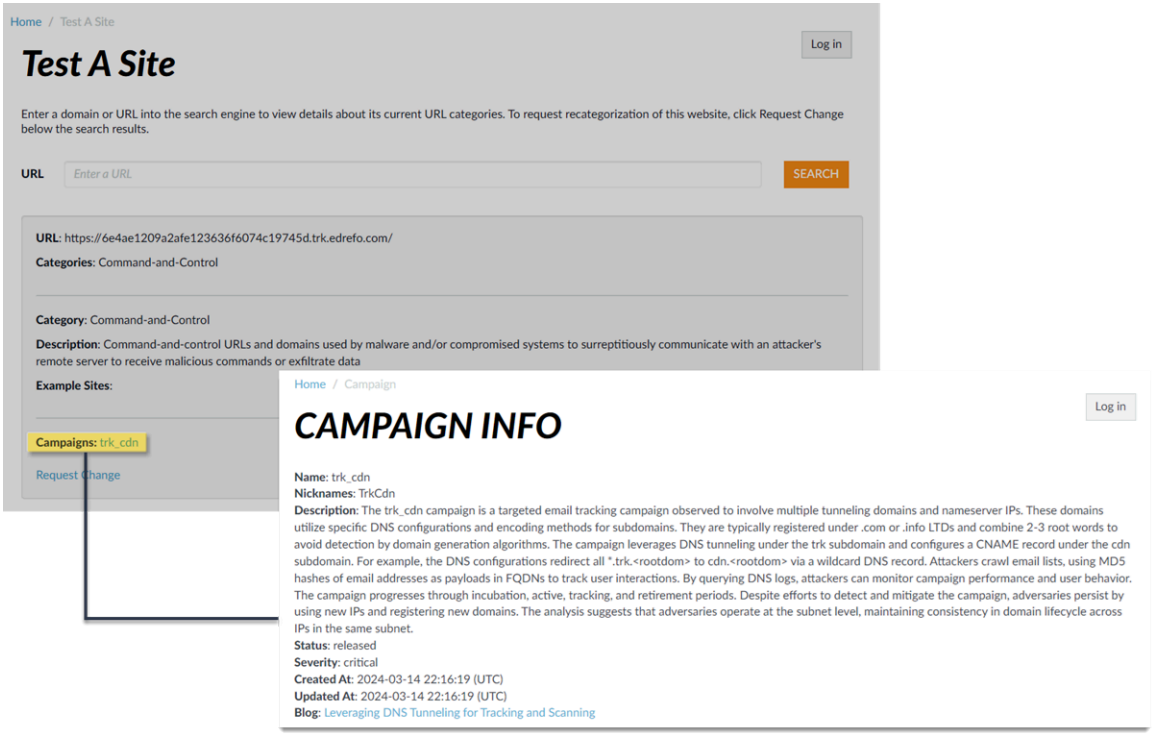
  1. PAN-OS



  2. ThreatVault

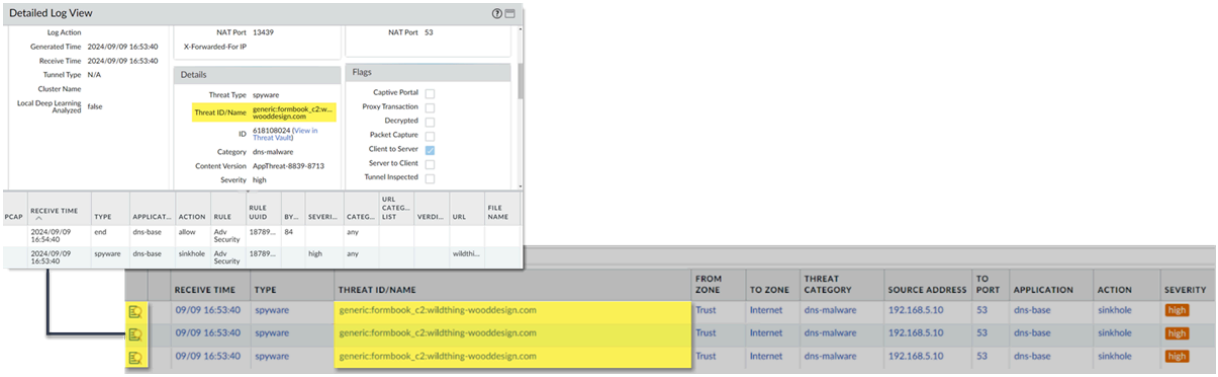


  3. URLフィルタリングTest-A-Site

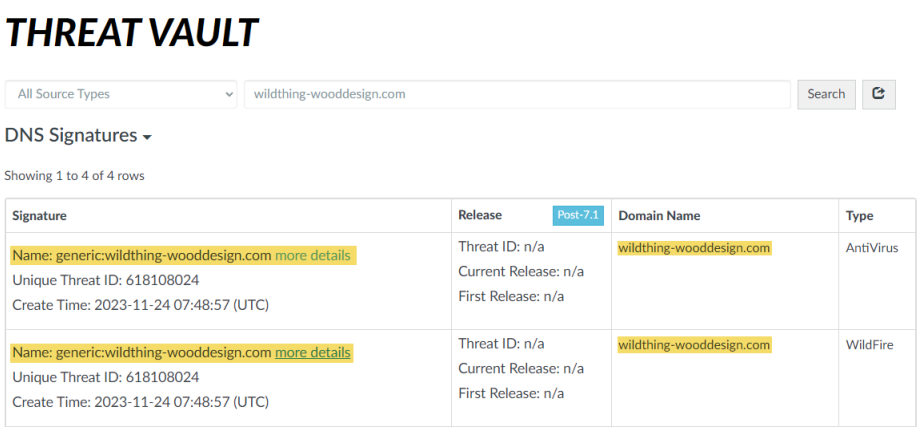


- 蓄積されたドメインの**APT**属性

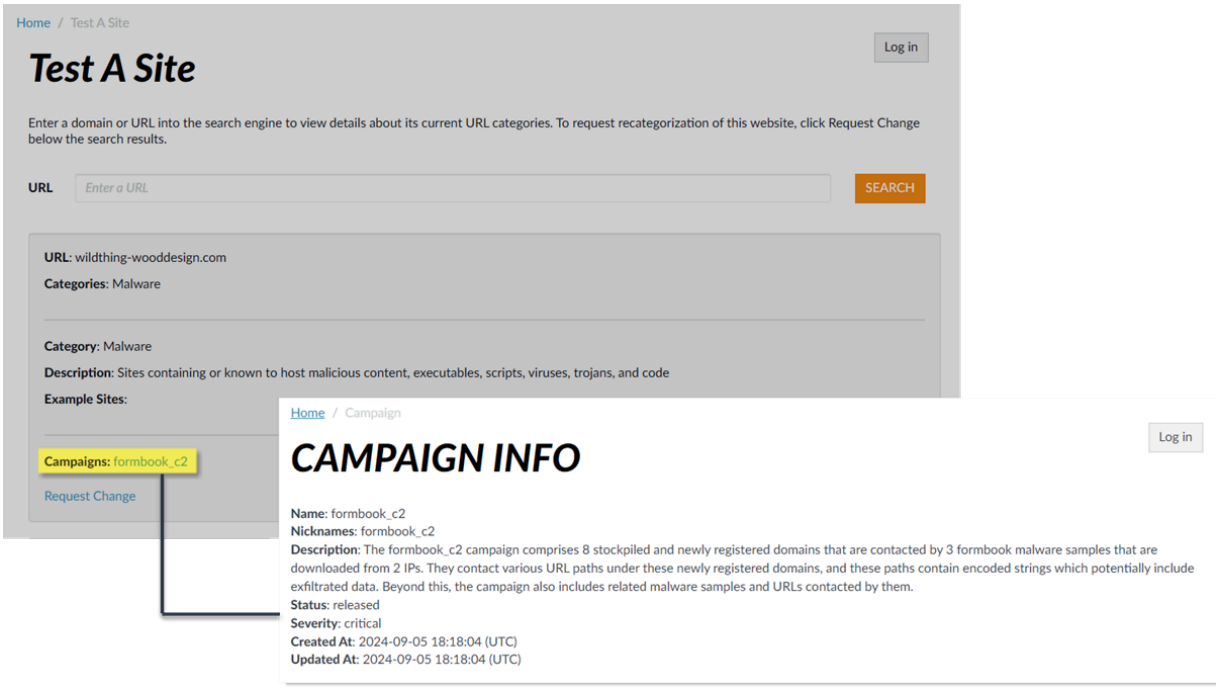
1. PAN-OS



2. ThreatVault



3. URLフィルタリングTest-A-Site



DNSセキュリティ ログの表示 (AIOps for NGFW Free)

*DNS*セキュリティで解析された問題のない*DNS*クエリは、*AIOps for NGFW Free*ログ ビューアーに表示されません。*Strata Logging Service*アプリにログインし、問題のない*DNS*ログ エントリにアクセスします。

STEP 1 | Palo Alto Networksのサポート アカウントに関連付けられた資格情報を使用し、ハブ上のAIOps for NGFW Freeアプリケーションにログインします。

STEP 2 | AIOps for NGFW FreeでDNSセキュリティを使用して処理されたDNSクエリを検索します。

1. **[Incidents and Alerts (インシデントとアラート)]** > **[Log Viewer (ログ ビューアー)]**を選択します。
2. 脅威フィルタを使用して検索を制限し、DNSカテゴリーに基づいてログ クエリを送信します。たとえば、`threat_category.value = 'dns-c2'`と指定すると、C2ドメインと判定されたログが表示されます。他のDNSタイプを検索するには、c2をサポートされている別のDNSカテゴリー（ddns、parking、malwareなど）に置き換えます。必要に応じて、追加のクエリ パラメータ (重大度レベルやサブタイプなど) や日付範囲など、検索条件を調整します。
3. ログ エントリを選択して、検出されたDNS脅威の詳細を表示します。
4. 脅威カテゴリー は、詳細ログ ビューの **[Details (詳細)]** ペインに表示されます。脅威に関するその他の関連詳細は、対応するウィンドウに表示されます。

DNSセキュリティ ログの表示 (Strata Logging Service)

STEP 1 | Palo Alto Networksのサポート アカウントに関連付けられた資格情報を使用し、ハブ上のStrata Logging Serviceアプリケーションにログインします。

STEP 2 | ログ タイプに基づいてストレージを割り当てます。Strata Logging ServiceのDNSセキュリティ ログに記憶域が割り当てられていない場合、Strata Logging Service経由でログ エントリを表示できません。

STEP 3 | Strata Logging ServiceでDNSセキュリティを使用して処理されたDNSクエリを検索します。

1. **[Explore (探索)]**を選択してStrata Logging Serviceログ ビューアーを開きます。
2. 脅威フィルタを使用して検索を制限し、DNSカテゴリーに基づいてログ クエリを送信します。たとえば、`threat_category.value = 'dns-c2'`と指定すると、C2ドメインと判定されたログが表示されます。他のDNSタイプを検索するには、c2をサポートされている別のDNSカテゴリー（ddns、parking、malwareなど）に置き換えます。必要に応じて、追加のクエリ パラメータ (重大度レベルやサブタイプなど) や日付範囲など、検索条件を調整します。
3. ログ エントリを選択して、検出されたDNS脅威の詳細を表示します。
4. 脅威カテゴリーは、詳細ログ ビューの**[Details (詳細)]**ペインに表示されます。脅威に関するその他の関連詳細は、対応するウィンドウに表示されます。