

The Palo Alto Networks logo, featuring a stylized orange and red icon to the left of the word "paloalto" in a lowercase, sans-serif font.

TECHDOCS

高度なDNSセキュリティ管理

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

Palo Alto Networks, Inc.

www.paloaltonetworks.com

© 2022-2022 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

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.....	5
クラウド配信型の DNS シグネチャおよび保護.....	8
データの収集とロギング.....	15
地域サービス ドメイン.....	17
DNSセキュリティ地域サービス ドメイン.....	17
Advanced DNSセキュリティ地域サービス ドメイン.....	18
DNSセキュリティ サブスクリプション サービスの設定.....	21
DNS セキュリティの有効化.....	23
Advanced DNSセキュリティの有効化.....	40
TLSを介したDNSセキュリティの設定.....	53
DoHによるDNSセキュリティの設定.....	55
ドメイン例外の作成と許可 ブロックリスト.....	58
テスト ドメイン.....	63
DNSセキュリティ クラウド サービスへの接続テスト.....	67
DNS セキュリティ.....	67
高度DNSセキュリティ.....	68
検索タイムアウトの設定.....	70
DNS セキュリティ.....	70
高度DNSセキュリティ.....	71
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.....	73
DNSセキュリティ サブスクリプション サービスの監視.....	77
DNSセキュリティ ダッシュボードの表示.....	79
DNSセキュリティ ダッシュボード カード.....	79
DNSセキュリティ ログの表示.....	88

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?
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> □ 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可能です。

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](#)

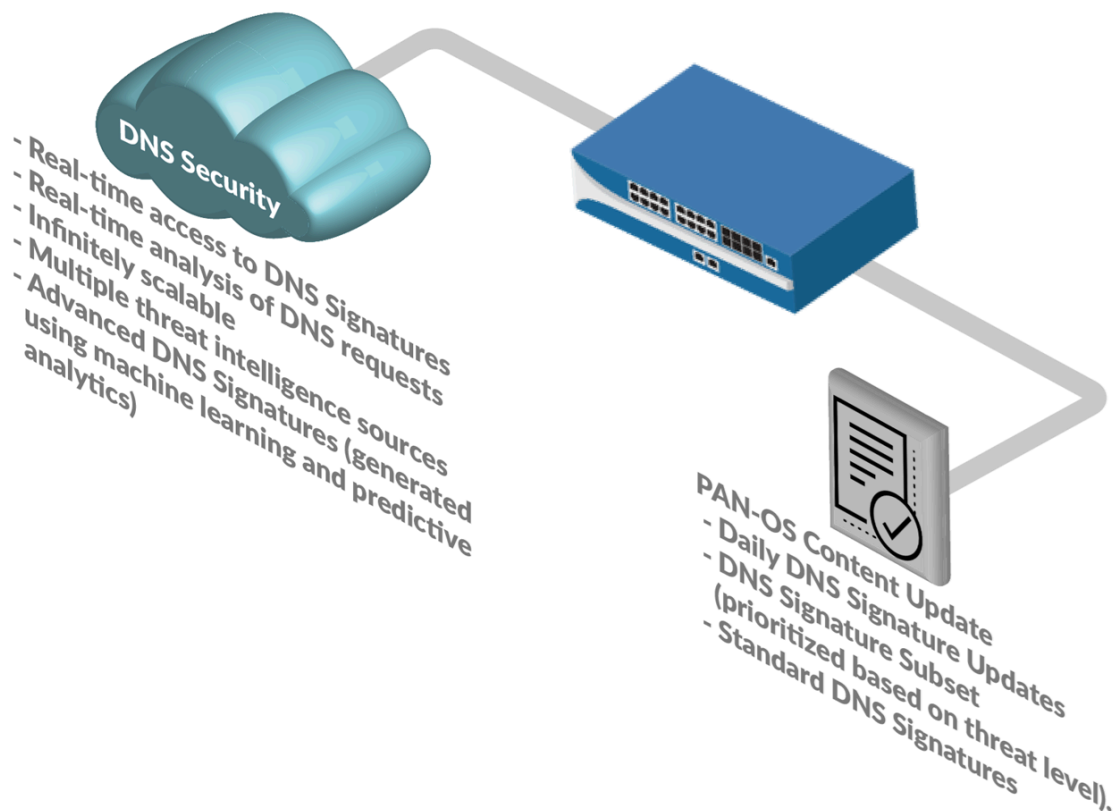
DNSセキュリティとAdvanced DNSセキュリティをネットワークにデプロイする方法をご紹介します。

- [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?
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> □ 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 シグネチャー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 チャン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 익스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 익스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 オペレーター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ムングによって正当な Web サイトになりますことにより、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 (ダンダリング **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)。
- 人気の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やウェブサイトにも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 ゾーンダンダリング(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も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も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?
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> □ 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、**commit** 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?
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> □ 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せん。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?
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> □ 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](#)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?
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> □ 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 (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 [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)]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。

best-practice



Configuration Profile Usage

Name * best-practice Description Best practice dns security profile

Security Rules Using This Profile 6

Profile Groups Containing This Profile 10

Name	Location	Action	Packet Capture
DNS Security (9)			
Grayware Domains	Predefined	sinkhole	disable
Newly Registered Domains	Predefined	sinkhole	disable
Parked Domains	Predefined	sinkhole	disable
Proxy Avoidance and Anonymizers	Predefined	sinkhole	disable
Ad Tracking Domains	Predefined	sinkhole	disable
Command and Control Domains	Predefined	sinkhole	extended-capture
Dynamic DNS Hosted Domains	Predefined	sinkhole	disable
Phishing Domains	Predefined	sinkhole	disable
Malware Domains	Predefined	sinkhole	disable

• Default Action

Overrides (0)

Override DNS Security for these domains or FQDNs. Delete Add Override

Domain/FQDN	Description
<input type="checkbox"/>	

DNS Sinkhole Settings

Sinkhole IPv4 pan-sinkhole-default-ip (Palo Alto Networks Sinkhole IP)

Sinkhole IPv6 ::1 (IPv6 Loopback IP)

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。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。

- （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。

Anti-Spyware Profile
ⓘ

Name: Best-Practice

Description:

Signature Policies
Signature Exceptions
DNS Policies
DNS Exceptions

DNS Policies

🔍 9 items → ×

SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
Palo Alto Networks Content			
<input type="checkbox"/> default-paloalto-dns		sinkhole	extended-capture
DNS Security			
<input type="checkbox"/> Command and Control Domains	default (high)	sinkhole	extended-capture
<input type="checkbox"/> Dynamic DNS Hosted Domains	default (informational)	sinkhole	disable
<input type="checkbox"/> Grayware Domains	default (low)	sinkhole	disable
<input type="checkbox"/> Malware Domains	default (medium)	sinkhole	disable
<input type="checkbox"/> Parked Domains	default (informational)	sinkhole	disable
<input type="checkbox"/> Phishing Domains	default (low)	sinkhole	disable
<input type="checkbox"/> Proxy Avoidance and Anonymizers	default (low)	sinkhole	disable
<input type="checkbox"/> Newly Registered Domains	default (informational)	sinkhole	disable

DNS Sinkhole Settings

Sinkhole IPv4: Palo Alto Networks Sinkhole IP (sinkhole.paloaltonetworks.com)

Sinkhole IPv6: IPv6 Loopback IP (::1)

Block DNS Record Types

SVCB (64) HTTPS (65) ANY (255)

OK
Cancel

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。

Anti-Spyware Profile

Name: Best-Practice
Description:

Signature Policies | Signature Exceptions | **DNS Policies** | DNS Exceptions

DNS Policies

SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
Palo Alto Networks Content			
default-paloalto-dns		sinkhole	extended-capture
DNS Security			
Command and Control Domains	default (high)	sinkhole	extended-capture
Dynamic DNS Hosted Domains	default (informational)	sinkhole	disable
Grayware Domains	default (low)	sinkhole	disable
Malware Domains	default (medium)	sinkhole	disable
Parked Domains	default (informational)	sinkhole	disable
Phishing Domains	default (low)	sinkhole	disable
Proxy Avoidance and Anonymizers	default (low)	sinkhole	disable
Newly Registered Domains	default (informational)	sinkhole	disable

DNS Sinkhole Settings

Sinkhole IPv4: Palo Alto Networks Sinkhole IP (sinkhole.paloaltonetworks.com)

Sinkhole IPv6: IPv6 Loopback IP (::1)

OK Cancel

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。

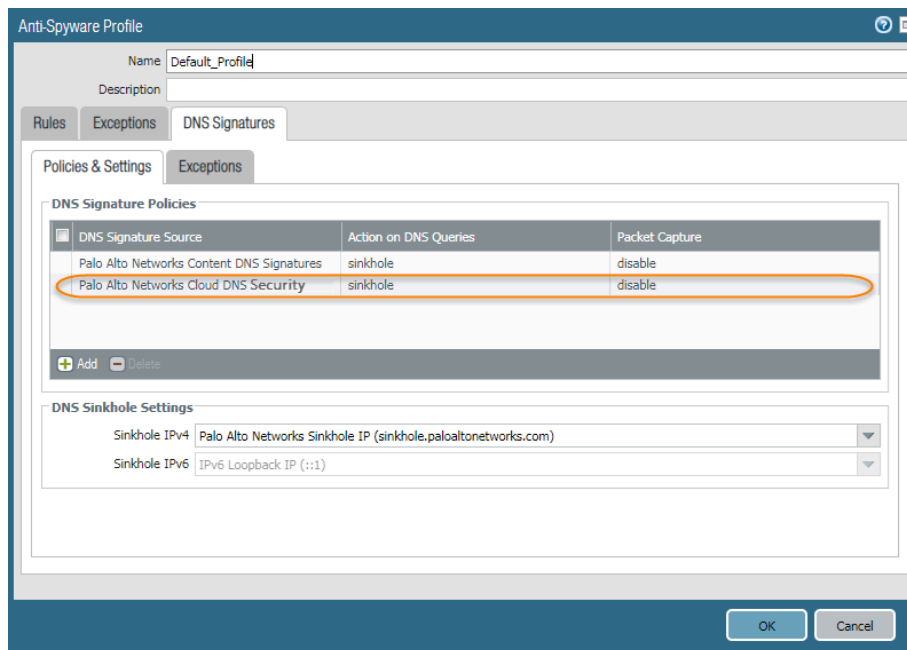
1. **Objects (オブジェクト) > Security Profiles (セキュリティ プロファイル) > Anti-Spyware (アンチスパイウェア)** を選択します。
2. 既存のプロファイルを変更あるいはプロファイルを作成するか、既存のデフォルトプロファイルの1つを選択してコピーします。
3. プロファイルに **Name (名前)** を付け、任意で説明を入力します。
4. **DNS Signatures (DNS シグネチャ) > Policies & Settings (ポリシーおよび設定)** タブを選択します。
5. **Palo Alto Networks 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?
<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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(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。

- 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。

DNS Categories (11)			
Name	Location	Action	Packet Capture
▼ DNS Security (9)			
Parked Domains	Predefined	sinkhole	disable
Proxy Avoidance and Anonymizers	Predefined	sinkhole	disable
Ad Tracking Domains	Predefined	sinkhole	disable
Command and Control Domains	Predefined	sinkhole	extended-capture
Dynamic DNS Hosted Domains	Predefined	sinkhole	disable
Phishing Domains	Predefined	sinkhole	disable
Malware Domains	Predefined	sinkhole	disable
▼ Advanced DNS Security (2)			
Dns Misconfiguration Domains	Predefined	• default (allow)	
Hijacking Domains	Predefined	• default (allow)	

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ーを

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 Misconfigurations (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。

DNS Zone Misconfigurations (0)	
Domain/FQDN	Description
+ -	

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」の後にカテゴリーが付けられます。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 カテゴリが使用されます。それらのインスタンスでは、カテゴリ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。

Misconfigured Domains	Misconfigured Reasons	Hits
youtube.com	QA dnsmisconfig test youtube.com:192.168.5.78	3
yougube.com	QA dnsmisconfig test yougube.com:192.168.5.77	0
misconfig.test.vnruser1	dnsmisconfig_zone test: misconfig.test.vnruser1	6
misconfig.test.vnruser	dnsmisconfig_zone test: misconfig.test.vnruser	21
misconfig.test.parul	dnsmisconfig_zone test: misconfig.test.parul	30
misconfig.test.adns123	dnsmisconfig_zone test: misconfig.test.adns123	12
misconfig.test.adns	dnsmisconfig_zone test: misconfig.test.adns	3

Displaying 1 - 7 of 7 Rows 10 Page 1 of 1

- **[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。

Hijacked	Hits
testpanw.com	12
malicious.test.adns	12
hijacking.test.vnr.com	18
hijacking.test.panw.com	50

Displaying 1 - 4 of 4 Rows 10 Page 1 of 1

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。

Advanced DNS Security	
Date Issued	December 29, 2023
Date Expires	January 29, 2024
Description	Advanced DNS Security Subscription

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。

The screenshot shows the 'Anti-Spyware Profile' configuration page. The 'DNS Policies' tab is selected, showing a table of DNS policies. The 'Advanced DNS Security' section is highlighted in yellow, showing policies for 'Dns Misconfiguration Domains' and 'Hijacking Domains'. Below the table, the 'DNS Zone Misconfigurations' section is empty.

SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
default-paloalto-dns		sinkhole	disable
DNS Security			
Ad Tracking Domains	default (informational)	default (allow)	disable
Command and Control Domains	default (high)	default (block)	disable
Dynamic DNS Hosted Domains	default (informational)	default (allow)	disable
Grayware Domains	default (low)	default (block)	disable
Malware Domains	default (medium)	default (block)	disable
Parked Domains	default (informational)	default (allow)	disable
Phishing Domains	default (low)	default (block)	disable
Proxy Avoidance and Anonymizers	default (low)	default (block)	disable
Newly Registered Domains	default (informational)	default (allow)	disable
Advanced DNS Security			
Dns Misconfiguration Domains	default (medium)	default (allow)	
Hijacking Domains	default (medium)	default (allow)	

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

リンクホール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。

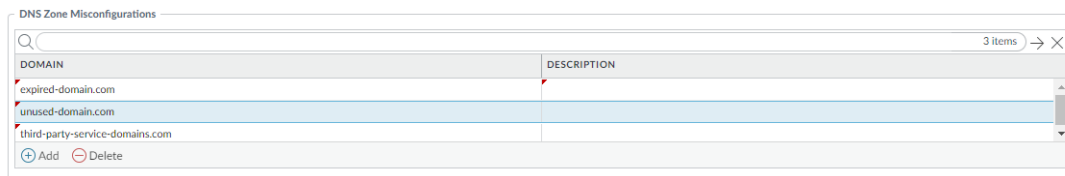
ログの重大度オプション:

- **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)]:** 直ちに脅威とははたらくても、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があります。
 - **[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 Misconfigurations (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

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が決定された場合、指定したカテゴリはプリフィックス「dns」の後にカテゴリ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 カテゴリに基づいてフィルタに付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。



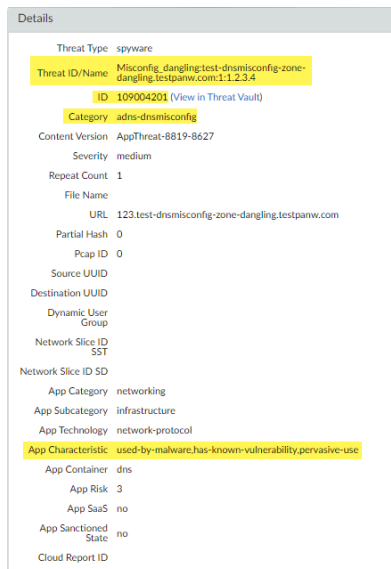
拡張されたAdvanced DNSセキュリティのリアルタイム解析を利用するには、PAN-OS 11.2以降を実行するファイアウォールを運用する必要があります。

- **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 カテゴリが使用されます。それらのインスタンスでは、カテゴリ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、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

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。

Misconfigured Domains	Misconfigured Reasons	Hits
youtube.com	QA dnsmisconfig test youtube.com:192.168.5.78	3
yougube.com	QA dnsmisconfig test yougube.com:192.168.5.77	0
misconfig.test.vnruser1	dnsmisconfig_zone test: misconfig.test.vnruser1	6
misconfig.test.vnruser	dnsmisconfig_zone test: misconfig.test.vnruser	21
misconfig.test.parul	dnsmisconfig_zone test: misconfig.test.parul	30
misconfig.test.adns123	dnsmisconfig_zone test: misconfig.test.adns123	12
misconfig.test.adns	dnsmisconfig_zone test: misconfig.test.adns	3

Displaying 1 - 7 of 7

Rows 10 Page 1 of 1

- [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。

Hijacked	Hits
testpanw.com	12
malicious.test.adns	12
hijacking.test.vnr.com	18
hijacking.test.panw.com	50

Displaying 1 - 4 of 4

Rows 10 Page 1 of 1

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?
<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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。
- [**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ず。

NAME	Source				Destination			URL CATEGORY	SERVICE	Decrypt Options					
	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE			ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNsuccessful 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?
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> □ 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 safely 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)

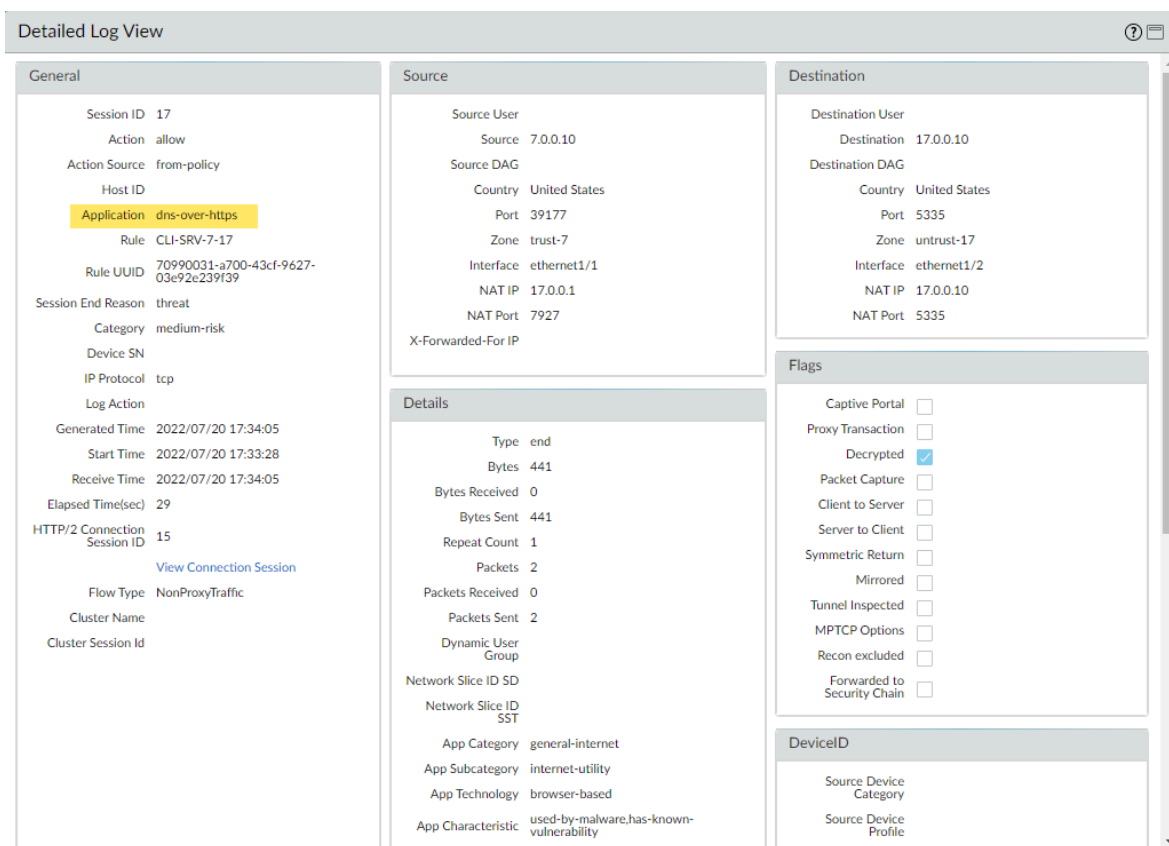
- STEP 1** | **PAN-OS Web インターフェイス**にログインします。
- STEP 2** | トラフィックを送受信できるようにするすべてのDoHリゾルバーを含む**カスタムURLカテゴリーリスト**を作成します (DNSサーバーのURLが必要です)。
- STEP 3** | 前のステップで作成したカスタムURLカテゴリー リストを参照する**復号ポリシー ルール**を作成します。
- STEP 4** | DoH要求の検査に使用する**アンチスパイウェア セキュリティ プロファイル**を更新または新規作成します。
- STEP 5** | **セキュリティ ポリシー 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。



The screenshot displays the 'Detailed Log View' interface with the following data:

General	Source	Destination
Session ID 17 Action allow Action Source from-policy Host ID Application dns-over-https Rule CLI-SRV-7-17 Rule UUID 70990031-a700-43cf-9627-03e92e239f39 Session End Reason threat Category medium-risk Device SN IP Protocol tcp Log Action Generated Time 2022/07/20 17:34:05 Start Time 2022/07/20 17:33:28 Receive Time 2022/07/20 17:34:05 Elapsed Time(sec) 29 HTTP/2 Connection Session ID 15 View Connection Session Flow Type NonProxyTraffic Cluster Name Cluster Session Id	Source User Source 7.0.0.10 Source DAG Country United States Port 39177 Zone trust-7 Interface ethernet1/1 NAT IP 17.0.0.1 NAT Port 7927 X-Forwarded-For IP	Destination User Destination 17.0.0.10 Destination DAG Country United States Port 5335 Zone untrust-17 Interface ethernet1/2 NAT IP 17.0.0.10 NAT Port 5335

Details
Type end Bytes 441 Bytes Received 0 Bytes Sent 441 Repeat Count 1 Packets 2 Packets Received 0 Packets Sent 2 Dynamic User Group Network Slice ID \$D Network Slice ID SST App Category general-internet App Subcategory internet-utility App Technology browser-based App Characteristic used-by-malware.has-known-vulnerability

Flags
Captive Portal <input type="checkbox"/> Proxy Transaction <input type="checkbox"/> Decrypted <input checked="" type="checkbox"/> Packet Capture <input type="checkbox"/> Client to Server <input type="checkbox"/> Server to Client <input type="checkbox"/> Symmetric Return <input type="checkbox"/> Mirrored <input type="checkbox"/> Tunnel Inspected <input type="checkbox"/> MPTCP Options <input type="checkbox"/> Recon excluded <input type="checkbox"/> Forwarded to Security Chain <input type="checkbox"/>

DeviceID
Source Device Category Source Device Profile

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?
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> □ 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。

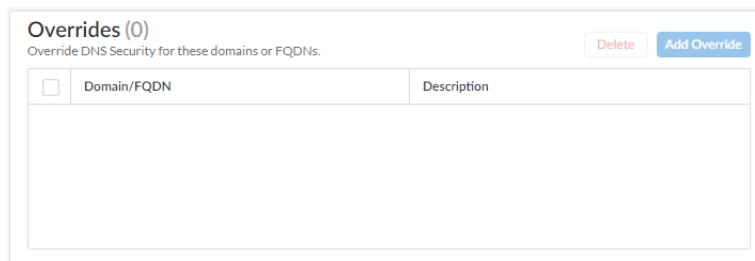
- [Strata Cloud Manager](#)
- [PAN-OS & Panorama](#)

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。

ENABLE	THREAT ID	DOMAIN/FQDN	THREAT NAME
<input checked="" type="checkbox"/>	193742436	evasion.fm	generic:evasion.fm
<input checked="" type="checkbox"/>	48958773	evasion-croisiere.com	generic:evasion-croisiere.com
<input checked="" type="checkbox"/>	20350128	EVASION-ONLINE.com	generic:EVASION-ONLINE.com
<input checked="" type="checkbox"/>	48956334	evasion-tech.com	generic:evasion-tech.com

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。

The screenshot shows the 'Anti-Spyware Profile' configuration window. The 'Name' field is set to 'Default_Profile'. The 'Description' field is empty. The 'DNS Exceptions' tab is selected. Below the tabs is a table titled 'DNS Domain/FQDN Allow List' with two columns: 'DOMAIN/FQDN' and 'DESCRIPTION'. One entry is present: 'example.email.paloaltonetworks.com' with the description 'Domain example description.'. Below the table are 'Add' and 'Delete' buttons. At the bottom right of the window are 'OK' and 'Cancel' buttons.

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。

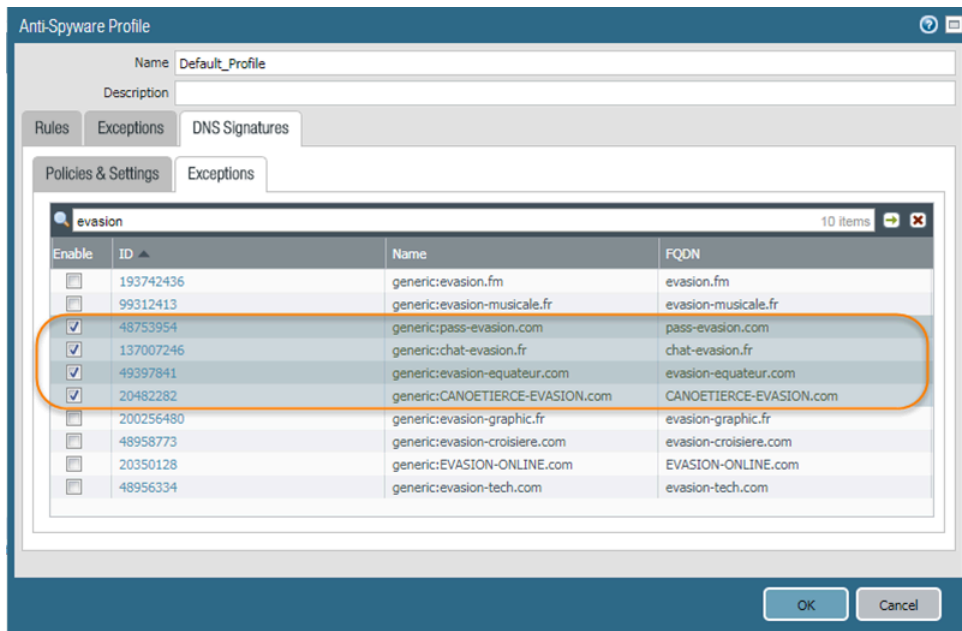
ドメイン例外の作成と許可 | ブロック リスト (PAN-OS 9.1)

 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?
<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">□ 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-rname.hijacking.testpanw.com	CNAME	1.test-cname-wc.hijacking.testpanw.com
test-cname-rname-wc.hijacking.testpanw.com	CNAME	1.test-cname-wildcard-1.hijacking.testpanw.com
*.test-cname-rname-sub-wc.hijacking.testpanw.com	CNAME	2.test-cname-wc.hijacking.testpanw.com
test-ns-rname.hijacking.testpanw.com	NS	test-ns.hijacking.testpanw.com
test-ns-rname-rdata-wc.hijacking.testpanw.com	NS	1.test-ns-wc.hijacking.testpanw.com
1.test-ns-rname-sub-wc.hijacking.testpanw.com	NS	test-ns.hijacking.testpanw.com
test-rname-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?
<ul style="list-style-type: none"> • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series 	<ul style="list-style-type: none"> □ 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?
<ul style="list-style-type: none"> • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series 	<ul style="list-style-type: none"> □ 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?
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> □ 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。

Name	Location	Source	Action	Packet Capture
DNS Security (9)				
Grayware Domains	Predefined	Palo Alto Networks Content	allow	disable
Newly Registered Domains	Predefined	Palo Alto Networks Content	default (allow)	disable
Parked Domains	Predefined	Palo Alto Networks Content	default (allow)	disable
Proxy Avoidance and Anonymizers	Predefined	Palo Alto Networks Content	allow	disable
Ad Tracking Domains	Predefined	Palo Alto Networks Content	default (allow)	disable
Command and Control Domains	Predefined	Palo Alto Networks Content	allow	disable
Dynamic DNS Hosted Domains	Predefined	Palo Alto Networks Content	default (allow)	disable
Phishing Domains	Predefined	Palo Alto Networks Content	allow	disable
Malware Domains	Predefined	Palo Alto Networks Content	allow	disable

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。

Overrides (0)

Override DNS Security for these domains or FQDNs. Delete Add Override

<input type="checkbox"/>	Domain/FQDN	Description

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。

Anti-Spyware Profile

Name: DNS-Security-Disabled

Description:

Signature Policies | Signature Exceptions | **DNS Policies** | DNS Exceptions | Inline Cloud Analysis

DNS Policies

▼ : DNS Security

Category	Log Severity	Action	Packet Capture
<input type="checkbox"/> Ad Tracking Domains	none	allow	disable
<input type="checkbox"/> Command and Control Domains	none	allow	disable
<input type="checkbox"/> Dynamic DNS Hosted Domains	none	allow	disable
<input type="checkbox"/> Grayware Domains	none	allow	disable
<input type="checkbox"/> Malware Domains	none	allow	disable
<input type="checkbox"/> Parked Domains	none	allow	disable
<input type="checkbox"/> Phishing Domains	none	allow	disable
<input type="checkbox"/> Proxy Avoidance and Anonymizers	none	allow	disable
<input type="checkbox"/> Newly Registered Domains	none	allow	disable

DNS Sinkhole Settings

Sinkhole IPv4: Palo Alto Networks Sinkhole IP (sinkhole.paloaltonetworks.com)

Sinkhole IPv6: IPv6 Loopback IP (::1)

Block DNS Record Types

SVCB HTTPS ANY

OK Cancel

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。

Signature Policies | Signature Exceptions | DNS Policies | **DNS Exceptions** | Inline Cloud Analysis

DNS Domain/FQDN Allow List

DOMAIN/FQDN	DESCRIPTION

+ Add - Delete

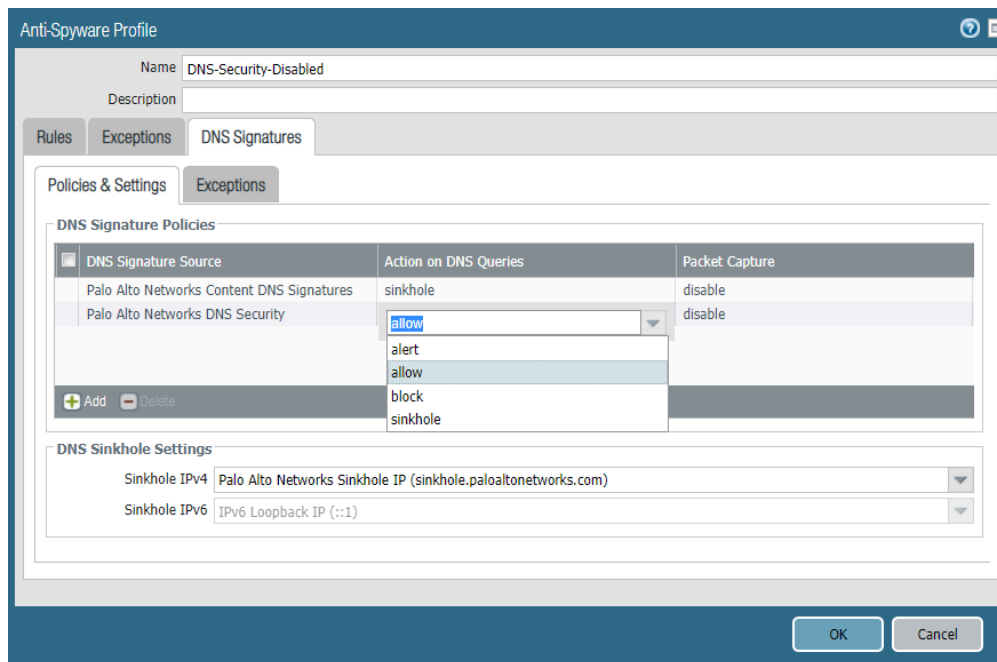
STEP 4 | **OK** をクリックし、アンチスパイウェア プロファイルを保存します。

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?
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> □ 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?
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> □ 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?
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> □ 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	<p>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。</p>  <ul style="list-style-type: none"> 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	<p>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。</p>  <ul style="list-style-type: none"> 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
サブスクリプション	<ul style="list-style-type: none"> DNSカテゴリ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。 <p>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。</p>  <ul style="list-style-type: none"> [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	<p>DNSカテゴリに基づく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。</p> <p>High-Risk DNS Category Trend</p> <p>Examine the trend of high-risk DNS requests according to DNS category. View trends according to the action enforced against the requests</p>  <ul style="list-style-type: none"> DNSカテゴリ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																																																				
	<ul style="list-style-type: none"> 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。 																																																				
<p>アクション間のDNSカテゴリーの配布</p>	<p>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。</p> <ul style="list-style-type: none"> 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。 <p>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。</p> <ul style="list-style-type: none"> 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。 <div data-bbox="621 1056 1455 1522" data-label="Figure"> <p>High Risk DNS Category Distribution across Actions Examine the action taken on DNS requests in each DNS category</p> <table border="1"> <thead> <tr> <th colspan="4">MALICIOUS</th> </tr> <tr> <th>Category</th> <th>Allow</th> <th>Blocked</th> <th>Sinkhole</th> </tr> </thead> <tbody> <tr> <td>Malware</td> <td>423</td> <td>423</td> <td>423</td> </tr> <tr> <td>Phishing</td> <td>423</td> <td>423</td> <td>423</td> </tr> <tr> <td>C2</td> <td>423</td> <td>423</td> <td>423</td> </tr> <tr> <td>Grayware</td> <td>423</td> <td>423</td> <td>423</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th colspan="4">OTHERS</th> </tr> <tr> <th>Category</th> <th>Allow</th> <th>Blocked</th> <th>Sinkhole</th> </tr> </thead> <tbody> <tr> <td>Exception List</td> <td>423</td> <td>423</td> <td>423</td> </tr> <tr> <td>Parked</td> <td>423</td> <td>423</td> <td>423</td> </tr> <tr> <td>Proxy</td> <td>423</td> <td>423</td> <td>423</td> </tr> <tr> <td>Dynamic DNS</td> <td>423</td> <td>423</td> <td>423</td> </tr> <tr> <td>Newly Registered</td> <td>423</td> <td>423</td> <td>423</td> </tr> </tbody> </table> </div> <ul style="list-style-type: none"> 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。 	MALICIOUS				Category	Allow	Blocked	Sinkhole	Malware	423	423	423	Phishing	423	423	423	C2	423	423	423	Grayware	423	423	423	OTHERS				Category	Allow	Blocked	Sinkhole	Exception List	423	423	423	Parked	423	423	423	Proxy	423	423	423	Dynamic DNS	423	423	423	Newly Registered	423	423	423
MALICIOUS																																																					
Category	Allow	Blocked	Sinkhole																																																		
Malware	423	423	423																																																		
Phishing	423	423	423																																																		
C2	423	423	423																																																		
Grayware	423	423	423																																																		
OTHERS																																																					
Category	Allow	Blocked	Sinkhole																																																		
Exception List	423	423	423																																																		
Parked	423	423	423																																																		
Proxy	423	423	423																																																		
Dynamic DNS	423	423	423																																																		
Newly Registered	423	423	423																																																		

カード名	詳説																																	
ドメイン	<p>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。</p> <p>Domains</p> <p>Learn more about the domains accessed in your network. See how your organization's domain access trends compare to those of other organizations.</p> <table border="1"> <tr> <td>Total Domains</td> <td>Domains Unique to organization</td> <td>Domains seen in same industry</td> <td>Domains seen in other industries</td> </tr> <tr> <td>34.8K</td> <td>5.2K</td> <td>443</td> <td>11</td> </tr> </table> <ul style="list-style-type: none"> 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。 	Total Domains	Domains Unique to organization	Domains seen in same industry	Domains seen in other industries	34.8K	5.2K	443	11																									
Total Domains	Domains Unique to organization	Domains seen in same industry	Domains seen in other industries																															
34.8K	5.2K	443	11																															
トップ10ドメイン	<p>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。</p> <p>TOP 10 DOMAINS</p> <p>View your top 10 most accessed domains. Check the category of the domains and make sure you're taking the appropriate action against them</p> <table border="1"> <thead> <tr> <th>Domain Name</th> <th>DNS Category</th> <th>Action Taken</th> </tr> </thead> <tbody> <tr> <td>domian.com</td> <td>Malware</td> <td>450 ● 300 ● 100 ● 50</td> </tr> <tr> <td>universal101.com</td> <td>C2</td> <td>350 ● 300 ● 100 ● 50</td> </tr> <tr> <td>google.com</td> <td>Dynamic DNS</td> <td>250 ● 300 ● 100 ● 50</td> </tr> <tr> <td>paloaltonetworks.com</td> <td>Phishing</td> <td>450 ● 300 ● 100 ● 50</td> </tr> <tr> <td>domian.com</td> <td>Grayware</td> <td>450 ● 300 ● 100 ● 50</td> </tr> <tr> <td>domian.com</td> <td>Exceptions List</td> <td>450 ● 300 ● 100 ● 50</td> </tr> <tr> <td>domian.com</td> <td>Malware</td> <td>450 ● 300 ● 100 ● 50</td> </tr> <tr> <td>domian.com</td> <td>Parked</td> <td>450 ● 300 ● 100 ● 50</td> </tr> <tr> <td>domian.com</td> <td>C2</td> <td>450 ● 300 ● 100 ● 50</td> </tr> <tr> <td>domian.com</td> <td>C2</td> <td>450 ● 300 ● 100 ● 50</td> </tr> </tbody> </table> <p style="text-align: right;">View All DNS Requests ></p>	Domain Name	DNS Category	Action Taken	domian.com	Malware	450 ● 300 ● 100 ● 50	universal101.com	C2	350 ● 300 ● 100 ● 50	google.com	Dynamic DNS	250 ● 300 ● 100 ● 50	paloaltonetworks.com	Phishing	450 ● 300 ● 100 ● 50	domian.com	Grayware	450 ● 300 ● 100 ● 50	domian.com	Exceptions List	450 ● 300 ● 100 ● 50	domian.com	Malware	450 ● 300 ● 100 ● 50	domian.com	Parked	450 ● 300 ● 100 ● 50	domian.com	C2	450 ● 300 ● 100 ● 50	domian.com	C2	450 ● 300 ● 100 ● 50
Domain Name	DNS Category	Action Taken																																
domian.com	Malware	450 ● 300 ● 100 ● 50																																
universal101.com	C2	350 ● 300 ● 100 ● 50																																
google.com	Dynamic DNS	250 ● 300 ● 100 ● 50																																
paloaltonetworks.com	Phishing	450 ● 300 ● 100 ● 50																																
domian.com	Grayware	450 ● 300 ● 100 ● 50																																
domian.com	Exceptions List	450 ● 300 ● 100 ● 50																																
domian.com	Malware	450 ● 300 ● 100 ● 50																																
domian.com	Parked	450 ● 300 ● 100 ● 50																																
domian.com	C2	450 ● 300 ● 100 ● 50																																
domian.com	C2	450 ● 300 ● 100 ● 50																																

カード名	詳説
	<ul style="list-style-type: none"> 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	<p>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。</p> <div data-bbox="630 590 1453 961" style="border: 1px solid #ccc; padding: 10px;"> <p>DNS Resolvers</p> <p>Monitor malicious and suspicious DNS resolution activity in your network. View the top DNS resolvers that resolve to malicious domains and the resolvers that are resolving a suspiciously low number of DNS requests.</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 48%;"> <p>TOP DNS RESOLVER IPS RESOLVING TO MALICIOUS DOMAINS</p> <div style="border-bottom: 1px solid #ccc; padding: 5px 0;"> <p>192.168.2.2 🔗</p> <p>Total Requests: #Count</p> <p>Malicious Domains: #Count</p> </div> <div style="text-align: right; margin-top: 5px;">View More details</div> <div style="border-bottom: 1px solid #ccc; padding: 5px 0;"> <p>135.156.2.23 🔗</p> <p>Total Requests: #Count</p> <p>Malicious Domains: #Count</p> </div> <div style="text-align: right; margin-top: 5px;">View Logs</div> <div style="padding: 5px 0;"> <p>164.123.235.2 🔗</p> <p>Total Requests: #Count</p> <p>Malicious Domains: #Count</p> </div> </div> <div style="width: 48%;"> <p>LEAST REQUESTED DNS RESOLVERS</p> <div style="border-bottom: 1px solid #ccc; padding: 5px 0;"> <p>334.168.255.265 🔗</p> <p>Total Requests: #Count</p> <p>Malicious Domains: #Count</p> </div> <div style="border-bottom: 1px solid #ccc; padding: 5px 0;"> <p>124.168.2.234 🔗</p> <p>Total Requests: #Count</p> <p>Malicious Domains: #Count</p> </div> <div style="padding: 5px 0;"> <p>134.168.233.255 🔗</p> <p>Total Requests: #Count</p> <p>Malicious Domains: #Count</p> </div> </div> </div> </div>
ドメインの設定ミス(Advanced DNSセキュリティ)	<p>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。</p>

カード名	詳説																								
	 <table border="1"> <thead> <tr> <th>Misconfigured Domains</th> <th>Misconfigured Reasons</th> <th>Hits</th> </tr> </thead> <tbody> <tr> <td>youtube.com</td> <td>QA dnsmisconfig test youtube.com:192.168.5.78</td> <td>3</td> </tr> <tr> <td>yougube.com</td> <td>QA dnsmisconfig test yougube.com:192.168.5.77</td> <td>0</td> </tr> <tr> <td>misconfig.test.vnruser1</td> <td>dnsmisconfig_zone test: misconfig.test.vnruser1</td> <td>6</td> </tr> <tr> <td>misconfig.test.vnruser</td> <td>dnsmisconfig_zone test: misconfig.test.vnruser</td> <td>21</td> </tr> <tr> <td>misconfig.test.parul</td> <td>dnsmisconfig_zone test: misconfig.test.parul</td> <td>30</td> </tr> <tr> <td>misconfig.test.adns123</td> <td>dnsmisconfig_zone test: misconfig.test.adns123</td> <td>12</td> </tr> <tr> <td>misconfig.test.adns</td> <td>dnsmisconfig_zone test: misconfig.test.adns</td> <td>3</td> </tr> </tbody> </table>	Misconfigured Domains	Misconfigured Reasons	Hits	youtube.com	QA dnsmisconfig test youtube.com:192.168.5.78	3	yougube.com	QA dnsmisconfig test yougube.com:192.168.5.77	0	misconfig.test.vnruser1	dnsmisconfig_zone test: misconfig.test.vnruser1	6	misconfig.test.vnruser	dnsmisconfig_zone test: misconfig.test.vnruser	21	misconfig.test.parul	dnsmisconfig_zone test: misconfig.test.parul	30	misconfig.test.adns123	dnsmisconfig_zone test: misconfig.test.adns123	12	misconfig.test.adns	dnsmisconfig_zone test: misconfig.test.adns	3
Misconfigured Domains	Misconfigured Reasons	Hits																							
youtube.com	QA dnsmisconfig test youtube.com:192.168.5.78	3																							
yougube.com	QA dnsmisconfig test yougube.com:192.168.5.77	0																							
misconfig.test.vnruser1	dnsmisconfig_zone test: misconfig.test.vnruser1	6																							
misconfig.test.vnruser	dnsmisconfig_zone test: misconfig.test.vnruser	21																							
misconfig.test.parul	dnsmisconfig_zone test: misconfig.test.parul	30																							
misconfig.test.adns123	dnsmisconfig_zone test: misconfig.test.adns123	12																							
misconfig.test.adns	dnsmisconfig_zone test: misconfig.test.adns	3																							
<p>ハイジャックされたドメイン (Advanced DNSセキュリティ)</p>	<p>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。</p>  <table border="1"> <thead> <tr> <th>Hijacked</th> <th>Hits</th> </tr> </thead> <tbody> <tr> <td>testpanw.com</td> <td>12</td> </tr> <tr> <td>malicious.test.adns</td> <td>12</td> </tr> <tr> <td>hijacking.test.vnr.com</td> <td>18</td> </tr> <tr> <td>hijacking.test.panw.com</td> <td>50</td> </tr> </tbody> </table>	Hijacked	Hits	testpanw.com	12	malicious.test.adns	12	hijacking.test.vnr.com	18	hijacking.test.panw.com	50														
Hijacked	Hits																								
testpanw.com	12																								
malicious.test.adns	12																								
hijacking.test.vnr.com	18																								
hijacking.test.panw.com	50																								

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。

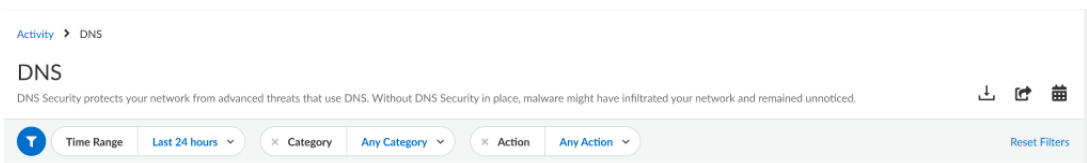
STEP 5 | ダッシュボード カードが提供するデータから、再コンテキスト化、インタラクション、ピボットを行うことができます。DNSセキュリティ ダッシュボードの各カードの概要については、「DNSセキュリティ ダッシュボード カード」を参照してください。


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)]、[Benign (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)]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?
<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> □ 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。

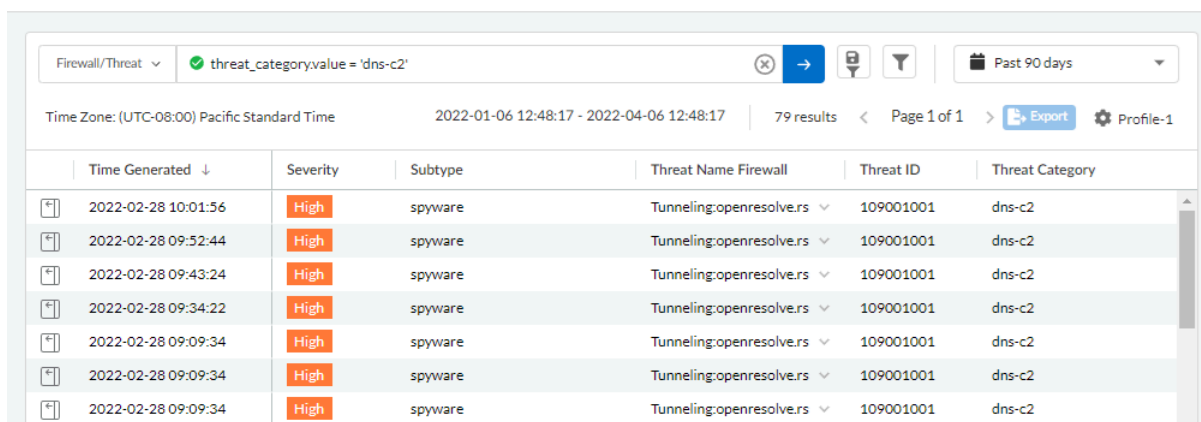
STEP 1 | Palo Alto Networksのサポート アカウントに関連付けられた資格情報を使用し、[ハブ上](#)のStrata Cloud Managerにログインします。








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。

Log Viewer

Your logs are automatically-generated and provide an audit trail for system, configuration, and network events. Network logs record all events where Prisma Access acts on your network traffic.



	Time Generated ↓	Severity	Subtype	Threat Name Firewall	Threat ID	Threat Category
	2022-02-28 10:01:56	High	spyware	Tunneling:openresolve.rs	109001001	dns-c2
	2022-02-28 09:52:44	High	spyware	Tunneling:openresolve.rs	109001001	dns-c2
	2022-02-28 09:43:24	High	spyware	Tunneling:openresolve.rs	109001001	dns-c2
	2022-02-28 09:34:22	High	spyware	Tunneling:openresolve.rs	109001001	dns-c2
	2022-02-28 09:09:34	High	spyware	Tunneling:openresolve.rs	109001001	dns-c2
	2022-02-28 09:09:34	High	spyware	Tunneling:openresolve.rs	109001001	dns-c2
	2022-02-28 09:09:34	High	spyware	Tunneling:openresolve.rs	109001001	dns-c2

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。

General		
Time Generated	Severity	Subtype
2022-02-28 10:01:56	High	spyware
Threat Name Firewall	Threat Category	Application
Tunneling:openresolve.rs	dns-c2	dns
Direction Of Attack	File Name	File Type
client to server	3-14-161-68.1646070799.tr.research.openresolve.rs	
URL Domain	Verdict	Action
		sinkhole

Details		
Threat ID	File Hash	Log Exported
109001001		false
Log Setting	Repeat Count	Sequence No
Cortex Data Lake	1	612103
Payload Protocol ID	HTTP Method	Prisma Access Location
-1	unknown	US East
File URL		

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。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。

Q (category-of-threatid eq dns-c2)

	RECEIVE TIME	TYPE	THREAT ID/NAME	THREAT CATEGORY	CONTENT VERSION	FROM ZONE	TO ZONE	SOURCE ADDRESS	ID
	03/31 10:49:04	spyware	DGA:fndslijfnds.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:35	spyware	DGA:jiajfdasvcxvczfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:25	spyware	DGA:jiajfdasvcxvczfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:10	spyware	DGA:jiajfdasvcxvczfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:00	spyware	DGA:jiajfdasvcxvczfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 10:48:38	spyware	DGA:www.7jla5zcx77.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 10:48:28	spyware	DGA:www.pmedpevnt3lgi4ps23njcp6.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。

Detailed Log View

General	Source	Destination
Session ID 787	Source User	Destination User
Action drop-packet	Source 7.0.0.10	Destination 17.0.0.10
Host ID	Source DAG	Destination DAG
Application dns	Country United States	Country United States
Rule CLI-SRV-7-17	Port 35378	Port 53
Rule UUID 70990031-a700-43cf-9627-03e92e239f39	Zone trust-7	Zone untrust-17
Device SN	Interface ethernet1/1	Interface ethernet1/2
IP Protocol udp	NAT IP 17.0.0.1	NAT IP 17.0.0.10
Log Action	NAT Port 20988	NAT Port 53
Generated Time 2022/03/31 10:49:04	X-Forwarded-For IP	
Receive Time 2022/03/31 10:49:04		
Tunnel Type N/A		

Details
Threat Type spyware
Threat ID/Name DGA:fhdsljfhds.com
ID 10900001 (View in Threat Vault)
Category dns-c2
Content Version AppThreat-0-0
Severity high
Repeat Count 1
File Name
URL fhdsljfhds.com
Partial Hash 0
Pcap ID 0
Dynamic User Group
Network Slice ID SST
Network Slice ID SD
App Category networking
App Subcategory infrastructure
App Technology network-protocol
App Characteristic used-by-malware,has-known-vulnerability,pervasive-use
App Container
App Risk 3

Flags
Captive Portal <input type="checkbox"/>
Proxy Transaction <input type="checkbox"/>
Decrypted <input type="checkbox"/>
Packet Capture <input type="checkbox"/>
Client to Server <input checked="" type="checkbox"/>
Server to Client <input type="checkbox"/>
Tunnel Inspected <input type="checkbox"/>

DeviceID
Source Device Category
Source Device Profile
Source Device Model
Source Device Vendor
Source Device OS Family
Source Device OS Version
Source Device Host
Source Device MAC
Destination Device Category

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。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

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

The screenshot shows the 'Detailed Log View' interface. On the left, there are fields for 'Receive Time' (2024/08/29 13:24:14), 'Tunnel Type' (N/A), 'Cluster Name', and 'Local Deep Learning Analyzed' (false). The main 'Details' pane shows: Threat Type: spyware; Threat ID/Name: Tunneling:trk_cdredinfo.com; ID: 109001001 (view in Threat Vault); Category: dns-c2; Content Version: AppThreat-8839-8713; Severity: high; Repeat Count: 1; File Name: IBI_6ad5a1209+2d612263. The 'Flags' pane on the right has several checkboxes: Captive Portal, Proxy Transaction, Decrypted, Packet Capture (checked), Client to Server (checked), Server to Client, and Tunnel Inspected. Below the details is a table with columns: RECEIVE TIME, TYPE, THREAT ID/NAME, FROM ZONE, TO ZONE, THREAT CATEGORY, SOURCE ADDRESS, TO PORT, APPLICATION, ACTION, SEVERITY. Three rows of log entries are visible, all for 'spyware' with threat ID '109001001' and 'High' severity.

2. ThreatVault

THREAT VAULT

All Source Types ▼ 109001001 Search 🔄

DNS Signatures ▼

Showing 1 to 1 of 1 rows

Signature	Release	Domain Name	Type
Name: Real-Time DNS Detection: DNS Tunneling more details Unique Threat ID: 109001001 Create Time: 2019-01-31 01:56:00 (UTC)	Post-7.1 Threat ID: n/a Current Release: n/a First Release: n/a		

3. URLフィルタリングTest-A-Site

Home / Test A Site Log in

Test A Site

Enter a domain or URL into the search engine to view details about its current URL categories. To request recategorization of this website, click Request Change below the search results.

URL SEARCH

URL: <https://6e4ae1209a2afe123636f6074c19745d.trk.edrefo.com/>

Categories: Command-and-Control

Category: Command-and-Control

Description: Command-and-control URLs and domains used by malware and/or compromised systems to surreptitiously communicate with an attacker's remote server to receive malicious commands or exfiltrate data

Example Sites:

Campaigns: trk_cdn

[Request Change](#)

Home / Campaign Log in

CAMPAIGN INFO

Name: trk_cdn
Nicknames: TrkCdn

Description: The trk_cdn campaign is a targeted email tracking campaign observed to involve multiple tunneling domains and nameserver IPs. These domains utilize specific DNS configurations and encoding methods for subdomains. They are typically registered under .com or .info LTDs and combine 2-3 root words to avoid detection by domain generation algorithms. The campaign leverages DNS tunneling under the trk subdomain and configures a CNAME record under the cdn subdomain. For example, the DNS configurations redirect all *.trk.<rootdom> to cdn.<rootdom> via a wildcard DNS record. Attackers crawl email lists, using MD5 hashes of email addresses as payloads in FQDNs to track user interactions. By querying DNS logs, attackers can monitor campaign performance and user behavior. The campaign progresses through incubation, active, tracking, and retirement periods. Despite efforts to detect and mitigate the campaign, adversaries persist by using new IPs and registering new domains. The analysis suggests that adversaries operate at the subnet level, maintaining consistency in domain lifecycle across IPs in the same subnet.

Status: released
Severity: critical
Created At: 2024-03-14 22:16:19 (UTC)
Updated At: 2024-03-14 22:16:19 (UTC)
Blog: [Leveraging DNS Tunneling for Tracking and Scanning](#)

蓄積されたドメインのAPT属性

1. PAN-OS

Detailed Log View

Log Action Generated Time: 2024/09/09 16:53:40 Receive Time: 2024/09/09 16:53:40 Tunnel Type: N/A Cluster Name: Local Deep Learning Analyzed: false	NAT Port: 13439 X-Forwarded-For IP: Details Threat Type: spyware Threat ID/Name: generic:formbook_c2-wildthing-wooddesign.com ID: 618108024 (View in Threat Vault) Category: dns-malware Content Version: AppThreat-8839-0713 Severity: High	NAT Port: 53 Flags Captive Portal: <input type="checkbox"/> Proxy Transaction: <input type="checkbox"/> Decrypted: <input type="checkbox"/> Packet Capture: <input type="checkbox"/> Client to Server: <input checked="" type="checkbox"/> Server to Client: <input type="checkbox"/> Tunnel Inspected: <input type="checkbox"/>
--	--	--

PCAP	RECEIVE TIME	TYPE	APPLICAT...	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG...	VERDI...	URL	FILE NAME
	2024/09/09 16:54:40	end	dns-base	allow	Adv Security	18789...	64	any					
	2024/09/09 16:53:40	spyware	dns-base	sinkhole	Adv Security	18789...		High	any			wildthi...	

	RECEIVE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	THREAT CATEGORY	SOURCE ADDRESS	TO PORT	APPLICATION	ACTION	SEVERITY
	09/09 16:53:40	spyware	generic:formbook_c2-wildthing-wooddesign.com	Trust	Internet	dns-malware	192.168.5.10	53	dns-base	sinkhole	High
	09/09 16:53:40	spyware	generic:formbook_c2-wildthing-wooddesign.com	Trust	Internet	dns-malware	192.168.5.10	53	dns-base	sinkhole	High
	09/09 16:53:40	spyware	generic:formbook_c2-wildthing-wooddesign.com	Trust	Internet	dns-malware	192.168.5.10	53	dns-base	sinkhole	High

2. ThreatVault

THREAT VAULT

All Source Types wildthing-wooddesign.com Search

DNS Signatures ▼

Showing 1 to 4 of 4 rows

Signature	Release	Domain Name	Type
Name: generic:wildthing-wooddesign.com more details Unique Threat ID: 618108024 Create Time: 2023-11-24 07:48:57 (UTC)	Post-7.1 Threat ID: n/a Current Release: n/a First Release: n/a	wildthing-wooddesign.com	AntiVirus
Name: generic:wildthing-wooddesign.com more details Unique Threat ID: 618108024 Create Time: 2023-11-24 07:48:57 (UTC)	Threat ID: n/a Current Release: n/a First Release: n/a	wildthing-wooddesign.com	WildFire

3. URLフィルタリング Test-A-Site

The screenshot shows the 'Test A Site' interface. At the top, there is a search bar with the text 'Enter a URL' and a 'SEARCH' button. Below the search bar, the results for the URL 'wildthing-wooddesign.com' are displayed, showing categories like 'Malware' and a description. A 'Request Change' button is visible. An inset window titled 'CAMPAIGN INFO' provides details for the 'formbook_c2' campaign, including its name, nicknames, description, status, severity, and creation/updated dates.

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（`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。

