Radware DefensePro DDoS Mitigation リリースノート

ソフトウェアバージョン 8.22.2

最終更新日：2020 年 8 月

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

目次

CONTENT **4**

リリースの概要 **4**

サポートされるプラットフォームとモジュール **4**

デバイス管理 **4**

ソフトウェアのアップグレード **4**

新機能 **5**

アンチスキャン保護 5

バースト攻撃保護 5

BDoS 保護の追加と拡張 6

BDoS リアルタイムシグネチャの構文の変更 6

オーバーブロッキング防止 6

ランダム化されたフラッドに対する BDoS 拡張 6

BDoS リアルタイムシグネチャ生成プロセスから DNS トラフィックが除外される 7

ブラックリストとホワイトリスト 7

じゅうたん爆撃保護ツールセット 8

スプーフィングされた SYN 攻撃からの保護 8

トラフィックフィルタの機能拡張 9

アンチスキャン拡張機能 10

接続 PPS 保護 11

DNS フラッド保護の機能強化 11

DNS リアルタイムシグネチャの構文の変更 11

地理位置情報保護ソリューション 11

On-Device TLS / SSL Mitigation 12

HTTPS フラッド保護 12

Radware ERT Active Attackers Feed 13

トラフィック フィルタ 14

パケット異常保護の追加 15

新しいパケット異常保護：誤った GRE バージョン（ID 126） 15

新しいパケット異常保護：無効な GRE ヘッダー（ID 128） 15

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

シグネチャ保護アプリケーション セキュリティの機能強化 15
ERT Security Update Service（SUS）のサポート 15
複雑なフィルタ 16
フィルタの追加コンテンツタイプ 16
フィルタの追加コンテンツパラメータ 16
シグニチャ保護アプリケーション セキュリティのシグニチャのための HTTP アクション 16
SYN フラッド保護のための透過型プロキシ認証 17
シグネチャ保護アプリケーション セキュリティによるポリシーごとの CDN サポート 18
接続制限保護の一時停止アクション 18
古い未確立セッションの宛先のリセット 19
大きない EDNS パケットを許可する 19
メッセージタイプ別の syslog 詳細レポートの有効化 19
イベントタイプ別の SNMP トラップの送信の有効化 19
TLS 1.3 および楕円曲線暗号化証明書のサポート 20
HTTPS 管理インターフェイスで使用される TLS バージョンを制御する CLI ベースのオプション 20
デバイス認証用 TACACS+ 20
ポリシーごとの CPU 使用率のモニタリング 20
BDoS および SYN フラッド保護のプロファイル単位の詳細レポート設定 21
同時セッションのモニタリング用の SNMP 01D 21
変更内容 21
フラグメント化されたトラフィックに対する BDoS Real-Time Signature の最適化 21
BDoS および DNS 保護のグローバル設定をプロファイル設定に移動 21
DNS フラッド保護のグローバル設定 22
Out-of-State Protection の猶予期間の設定オプション 22
パケット異常保護の機能拡張：認識不能 L2 フォーマット（ID 100） 23
複数のパケットレポート宛先 23
NTP 設定 23
SNMPv3 セキュリティのための 128 ビット暗号化 23
SSH の強力な暗号化方式 23

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

ハッシュ化されたパスワードを使用しないファイル生成のサポート 24
その他の機能拡張..... 24
既知の制限事項..... 24
関連資料..... 25

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

CONTENT

Radware は、Cisco Firepower 用の Radware DefensePro DDoS Mitigation バージョン 8.22.2.0 のリリースを発表しました。

このリリースノートでは、Radware DefensePro DDoS Mitigation の前回のリリースバージョンである 8.13.01 以降の新機能とメンテナンス修正について説明します。

リリースの概要

バージョン 8.22.2.0 では、アンチスキャン保護、バースト攻撃保護、接続 PPS 保護、トラフィックフィルタなど、多くの新機能と拡張機能が導入されています。

リリース日：2020 年 8 月

ビルド番号：27

サポートされるプラットフォームとモジュール

このソフトウェアバージョンは、次のプラットフォームでサポートされています。

製品	プラットフォーム	SME	DME
Radware DefensePro DDoS Mitigation	仮想	ソフトウェアベース	非対応

デバイス管理

このバージョンの Radware DefensePro DDoS Mitigation は、APSolute Vision バージョン

4.60.00 を使用してテストされました。以前のバージョンの APSolute Vision を使用している場合は、バージョン 4.60.00 以降にアップグレードすることをお勧めします。

ソフトウェアのアップグレード

バージョン 8.22.2.0 への直接アップグレードは、Radware DefensePro DDoS Mitigation バージョン 8.13.01 からサポートされています。

Radware DefensePro DDoS Mitigation バージョンのアップグレードは、Firepower Chassis Manager を使用して、次のように行います。

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

1. [論理デバイス（Logical Devices）] をクリックします。[論理デバイスリスト（Logical Device List）] が表示されます。
2. アップグレードするセキュリティモジュールと Radware DefensePro DDoS Mitigation アプリケーションを選択します。
3. [バージョン設定（Set version）] を選択します。[イメージバージョンの更新（Update image version）] ウィンドウが表示されます。
4. 新しいバージョンである 8.22.2.0、使用する [リソースプロファイル（Resource Profile）] を選択し、[OK] をクリックします。

新機能

このセクションでは、バージョン 8.22.2.0 の新機能について説明します。

アンチスキャン保護

アンチスキャン機能は、ゼロデイ自己増殖型ネットワークワーム、ポートスキャン、および IP アドレススキャンなどの悪意のあるスキャンアクティビティから保護します。

アンチスキャン保護が有効になっている場合、攻撃を検出すると、事前定義された初期ブロッキング期間の間、ブロッキング フットプリント ルールを実装します。同じ送信元から繰り返しスキャンアクティビティが識別されると、ブロック期間が延長されます。

バースト攻撃保護

ヒットアンドラン DDoS とも呼ばれるバースト攻撃は、ランダムな間隔で大量の短いバースト攻撃を繰り返し実行します。各ショートバーストは数秒程度しか続きませんが、1 秒あたり数百ギガビットのスループットに達することがあります。

このバージョンでは、バースト攻撃から保護するために次の機能を組み合わせています。

- ランダムな間隔で数秒間続くことがある、秒単位の大量のバースト攻撃を軽減します。
- 攻撃トラフィックをブロックするシグネチャを自動的に作成し、正規のトラフィックを通過させます。
- バースト全体で変化する複数の攻撃ベクトルに動的に適応します。
- 誤検出を最小限に抑えます。

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

BDoS 保護の追加と拡張

BDoS リアルタイムシグネチャの構文の変更

[中程度（Medium）] の厳密性のリアルタイムシグネチャの構文が変更され、正規のトラフィックに対する攻撃トラフィックの検出精度が向上しました。[フットプリントの厳密性（Footprint Strictness）] が [中程度（Medium）] の新しい構文では、BDoS リアルタイムシグネチャを表す最上位のブール式で、少なくとも 1 つのブール AND 条件が存在する必要があり、ブール OR 条件は使用できません。

次に例を示します。

- AAND B
- (A OR B OR C) AND D AND E

  ここで、「(A OR B OR C)」はネストされた式です。

オーバーブロッキング防止

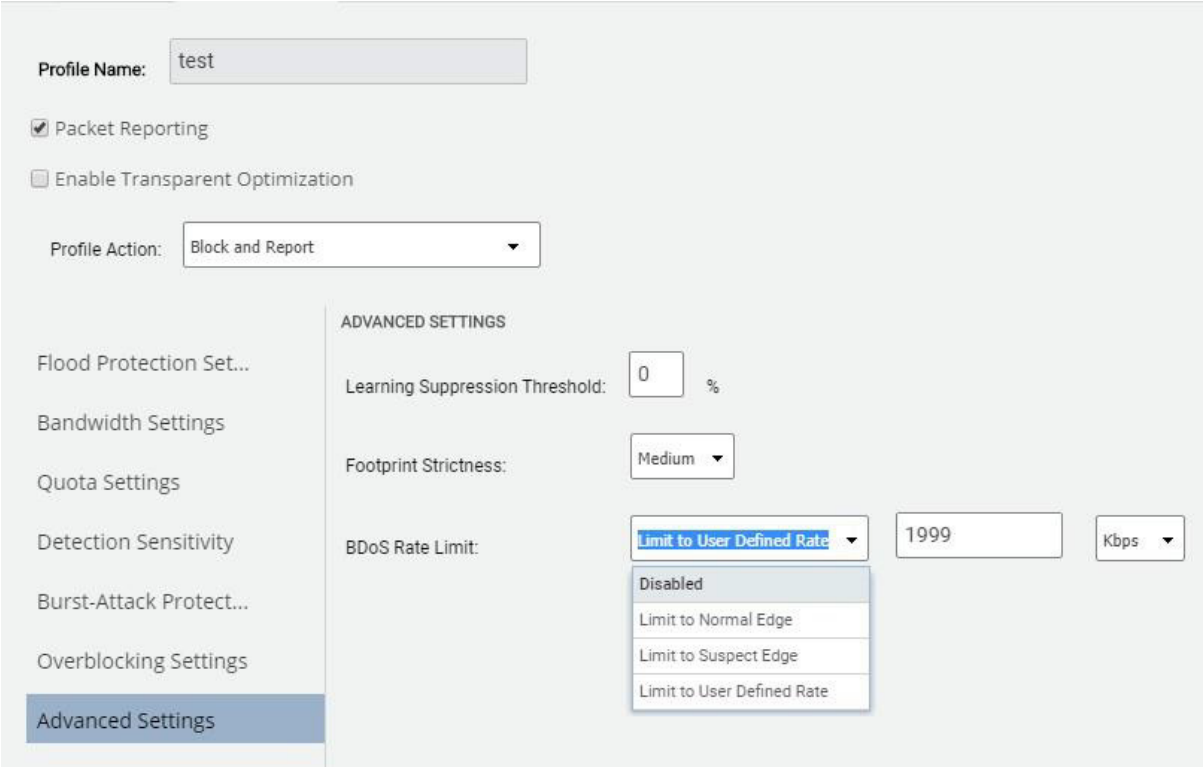
オーバーブロッキング防止を有効にすると、BDoS プロファイルが指定された厳密性レベルに一致するすべての必須条件を満たすシグネチャを作成して攻撃をブロックするが、この緩和によって一部の正規のトラフィックもブロックされるという状況に対処できます。

ランダム化されたフラッドに対する BDoS 拡張

BDoS は、高度な機械学習技術を使用して、ネットワーク層のボリューム攻撃を検出、分析、および軽減します。ランダム化攻撃は、本来、正規のトラフィックを模倣して検出を回避するように設計されています。レート制限への BDoS 保護のフォールバックにより、DefensePro は、特定の状況下でのみ、BDoS ベースラインに基づいてトラフィックを自動的にレート制限することで、このような高度な攻撃に対する追加の保護レイヤを適用できます。

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

図 1：ランダム化されたフラッドに対する BDoS 拡張



BDoS リアルタイムシグネチャ生成プロセスから DNS トラフィックが除外される

このバージョン以降、DNS フラッド保護が有効になっている場合、BDoS 保護は、BDoS リアルタイムシグネチャを生成するためのトラフィックを評価する間に DNS トラフィックを考慮しません。

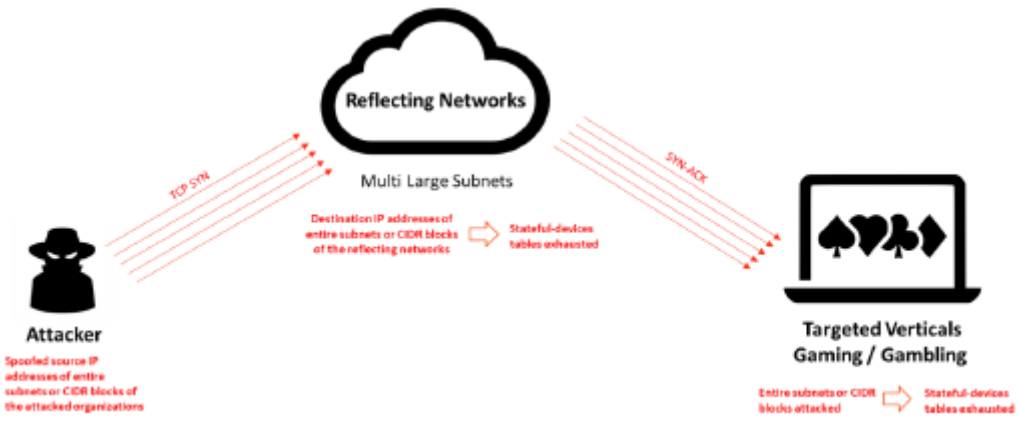
ブラックリストとホワイトリスト

Radware DefensePro DDoS Mitigation は、データトラフィック用の**ブラックリスト**および**ホワイトリスト**のルールを提供するようになりました。**ブラックリスト**は、デバイスがインスペクションなしで常にブロックするトラフィックで構成されます。**ブラックリスト**は、ネットワークポリシーのポリシー例外として使用します。**ホワイトリスト**は、セキュリティ インスペクションから除外されるトラフィックを決定します。

© 2020 Cisco I Radware. All rights reserved. This document is Cisco Public

じゅうたん爆撃保護ツールセット

このリリースでは、攻撃者の間でますます一般的になりつつある攻撃手法（じゅうたん爆撃）から組織を保護するための一連のツールが追加されています。じゅうたん爆撃攻撃は、スプーフィング攻撃、リフレクション攻撃、およびアンプ攻撃などの既知の攻撃戦術を組み合わせて、起動に必要な火力が少なく、同時に検出、特性評価、および緩和が困難な攻撃を生成します。



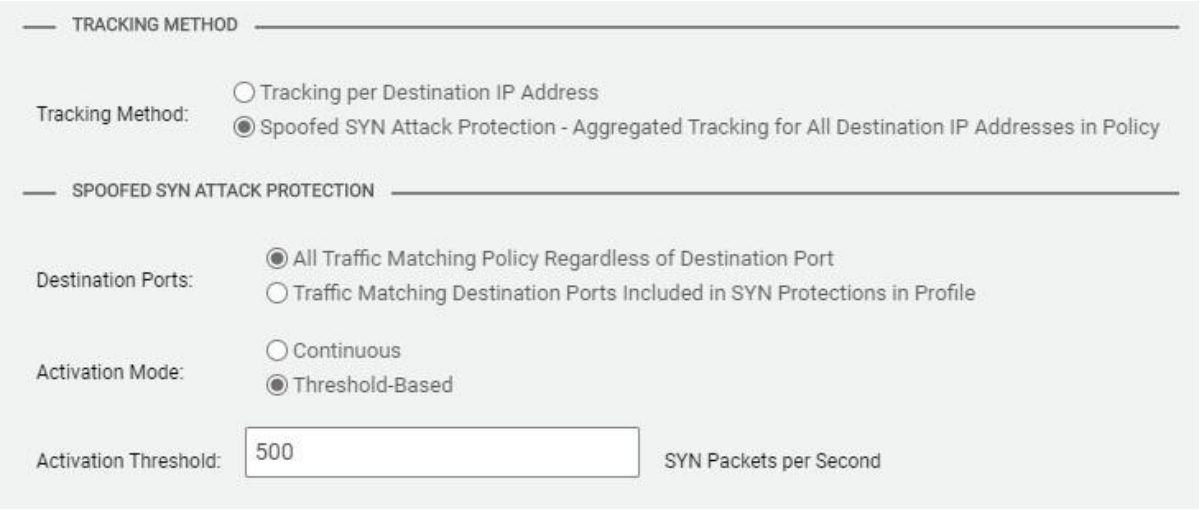
スプーフィングされた SYN 攻撃からの保護

スプーフィングされた SYN フラッドのじゅうたん爆撃攻撃は、一般的に被害者ネットワーク内の 1 つまたは特定の重要なサーバーに集中する通常の*単なる* SYN フラッド攻撃とは異なります。スプーフィングされた SYN フラッドじゅうたん爆撃攻撃は、保護されたネットワークに含まれる多数のランダムな宛先 IP アドレスに大量のジャンクトラフィックを送信し、複数のサブネットからの送信元を装うことにより、TCP リフレクションとアンプを利用します。このような攻撃は、一般的に保護されたサーバー内の個々の宛先サーバーに送信されるトラフィックの量を追跡する、アンチ DDoS ソリューションに見つからずに行われる可能性があります。このようなアンチ DDoS ソリューションは、DNS、HTTP、HTTPS、C-LDAP などのさまざまなプロトコルを使用し、保護されたネットワークの IP アドレスの多くまたはすべてを標的とする、よくできた分散型攻撃を区別できない可能性があります。

このバージョンの Radware DefensePro DDoS Mitigation では、SYN フラッド保護に加えて、「スプーフィングされた SYN 攻撃からの保護」が導入されています。スプーフィングされた SYN 攻撃からの保護は、複数のスプーフィングされた送信元 IP アドレスを使用し、宛先サブネットや CIDR 全体を標的とする攻撃を処理します。

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

図 2： スプーフィングされた SYN 攻撃からの保護



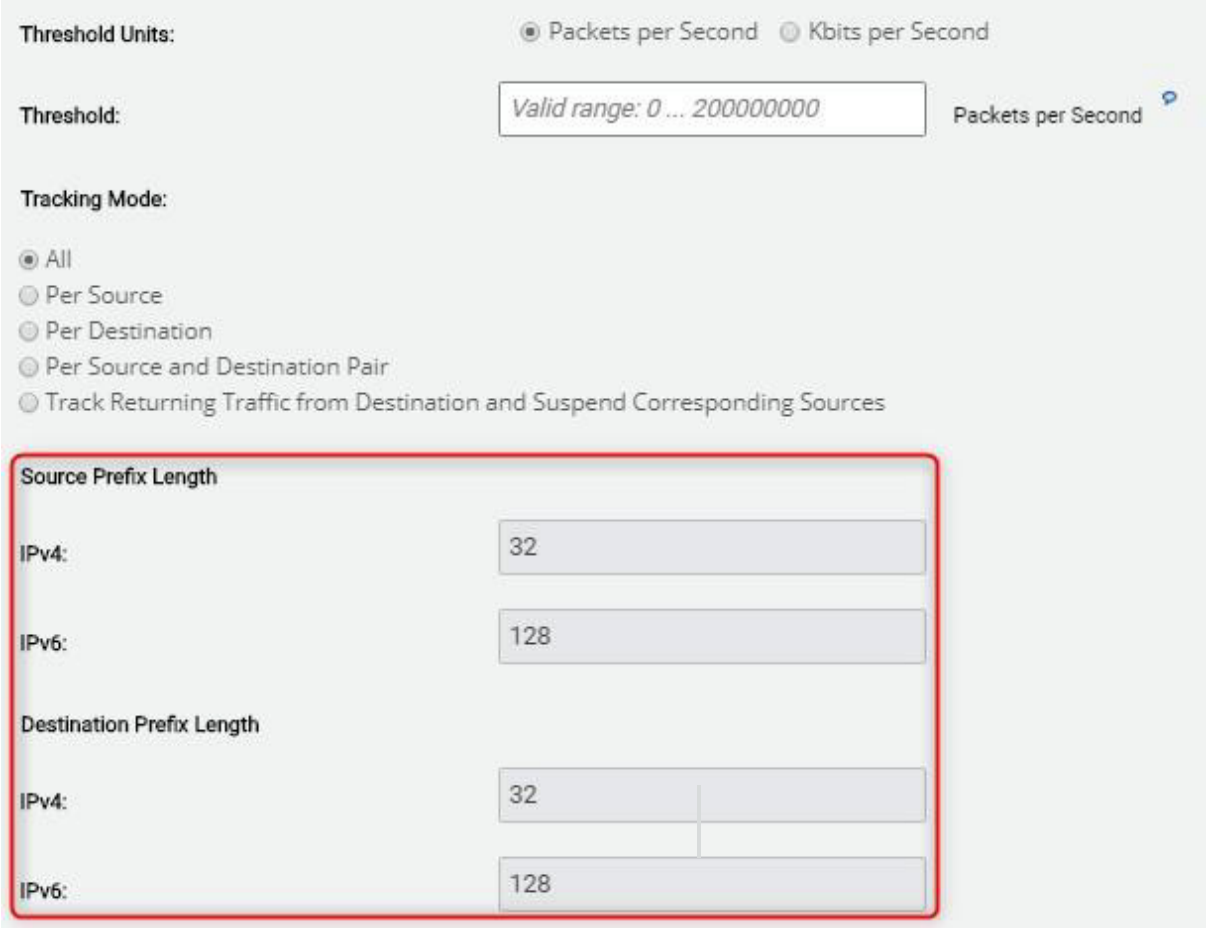
トラフィックフィルタの機能拡張

悪意のある攻撃者がじゅうたん爆撃攻撃で使用する戦術の 1 つは、リフレクションおよびアンプ効果のためにフルサブネットを使用し、個々の送信元が比較的少量のトラフィックを送信することです。このシナリオでは、送信元ごとのレート制限を使用する保護対策は効果的ではありません。これは、高いしきい値を使用しても送信元あたりの低レートのトラフィックは検出されず、低いしきい値を使用すると誤検出が発生し、正規のユーザーに悪影響を及ぼす可能性があるためです。

じゅうたん爆撃攻撃に対処する際のこの制限を克服するために、トラフィックフィルタでは、保護のニーズに合わせてトラッキング方法を選択できるようになりました。既存の個別の送信元または宛先 IP アドレストラッキング方式に加えて、送信元サブネットごと、または宛先サブネットごとにトラッキングを選択できるようになりました。この機能強化の目的は、サブネットから発信される大量のトラフィックを検出できるようにすることです。個々の送信元 IP アドレスは、送信元ごとの検出を回避するために少量のトラフィックを送信します。

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

図 3：トラフィックフィルタの機能拡張



アンチスキャン拡張機能

アンチスキャンとは、スキャンおよび偵察攻撃に対する堅牢な動作保護です。スキャン技術は、攻撃者によって、潜在的な被害者に対する攻撃前の調査として使用されます。攻撃者は、目標を達成するために、実際の IP アドレスを使用してプローブの試行に対する応答を受信します。

前述のように、じゅうたん爆撃攻撃で使用される戦術の 1 つは、悪意のある行為者それぞれが平均して少数のパケットを生成するような大きなサブネットを利用することです。この意味で、SYN ベースのじゅうたん爆撃攻撃は、リフレクタ側または被害者ネットワーク側での分散スキャン攻撃と見なすことができます。このバージョンでは、アンチスキャンが強化され、複数の送信元から発生する分散型スキャン攻撃を軽減できるようになりました。

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

接続 PPS 保護

このリリースの Radware DefensePro DDoS Mitigation では、接続ベースのフラッド攻撃を軽減することを目的とした接続 PPS 保護が導入されています。この保護により、接続ごとのパケット/秒レートを追跡して制限できるため、確立された接続から発生する悪意のあるアクティビティを排除できます。

接続 PPS プロファイルは、単一の保護ポリシー内できめ細かな保護を提供し、複数の個別の PPS 保護を設定できます。各 PPS 保護は、特定のトランスポートプロトコル（TCP および/または UDP、宛先 IP アドレス、および宛先ポート）に適用するように設定されます。

DNS フラッド保護の機能強化

DNS リアルタイムシグネチャの構文の変更

[中程度（Medium）] の厳密性のリアルタイムシグネチャの構文が変更され、正規のトラフィックに対する攻撃トラフィックの検出精度が向上しました。[フットプリントの厳密性（Footprint Strictness）] が [中程度（Medium）] の新しい構文では、DNS リアルタイムシグネチャを表す最上位のブール式で、少なくとも 1 つのブール AND 条件が存在する必要があり、ブール OR 条件は使用できません。

次に例を示します。

- AAND B
- (A OR B OR C) AND D AND E
  ここで、「(A OR B OR C)」はネストされた式です。

地理位置情報保護ソリューション

Radware の地理位置情報保護ソリューションは、ライブマップとフィードを使用して、DDoS 攻撃の上位国を可視化します。APSolute Vision Analytics のボタンをクリックするだけで、特定の国からのトラフィックをすぐにブロックできます。新しい専用攻撃マップを使用すると、上位の攻撃国が表示されます。

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

この緩和ソリューションでは、必要性と現在の脅威の状況またはビジネス要件に応じて、次の 2 つのモードのブロックアクティブ化を実行できます。

- 許可された国のリストまたはブロックされた国のリストの **Always-active-Persistent** 設定。これは、地理位置情報プロファイルを使用して行われます。
- 設定可能な期間の**オンデマンド**での一時的な国のブロッキング。これは、APSolute Vision Analytics の新しい*地理位置情報マップを使用して行われます。*

地理位置情報保護は、ポリシーごとのブロック/許可リストの設定をサポートします。これにより、キャリアとサービスプロバイダーは、テナントの国ブロックと許可リストを迅速に設定できるようになり、マルチテナントネットワークに最適なソリューションとなります。

地理位置情報保護には、ERT Silver Protection Package または ERT Gold Protection Package へのアクティブなサブスクリプションが必要です。ERT Silver Protection Package には、Security Update Subscription、ERT Active Attackers Subscription、および Geolocation Subscription が含まれています。ERT Gold Protection Package には、ERT Silver Protection Package と ERT Under Attack Service が含まれています。

On-Device TLS / SSL Mitigation

このバージョンの Radware DefensePro DDoS Mitigation では、DefenseSSL とも呼ばれるソフトウェアベースのオンデバイス TLS/SSL 緩和機能がサポートされます。*DefenseSSL は、Radware の特許取得済みの SSL 攻撃緩和ソリューションです。*

DefenseSSL は、SSL ベースの DDoS 攻撃に対する広範なカバレッジと最小の遅延により、最も効率的な SSL 攻撃保護を提供します。

オンデバイス SSL/TLS 緩和機能では、シンプルなワンボックス導入モデルを選択して、クリアテキストおよび TLS/SSL 暗号化ボリューム攻撃から保護することができます。

HTTPS フラッド保護

このバージョンでは、HTTPS プロトコルを介したフラッド攻撃から保護するために、HTTPS フラッド保護が導入されています。この保護では、革新的なアルゴリズムを使用して、トラフィックの復号化を最小限に抑えながら、攻撃の検出、攻撃元の特性評価、および攻撃の軽減を最も効率的な方法で実現します。

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

HTTPS フラッド保護には次の段階があります。

1. **攻撃検出：HTTPS** フラッド攻撃は、トラフィックの復号化を必要としない革新的な独自のアルゴリズムを使用して検出されます。Radware DefensePro DDoS Mitigation は、平時の HTTPS トラフィックのベースラインを確立し、学習したベースラインからの逸脱に基づいて攻撃を検出すると同時に、フラッシュクラウドなど、トラフィック量の正規の一時的な増加を許可します。

2. **攻撃元の特性評価：**特性評価の段階で、Radware DefensePro DDoS Mitigation は、その革新的なアルゴリズムを使用して、正規の送信元と攻撃者と疑われる送信元を区別します。前述の攻撃検出段階と同様に、攻撃元の特性評価段階ではトラフィックの復号化は必要ありません。この段階では、Radware DefensePro DDoS Mitigation により、疑わしいソース攻撃元のリストが作成され、攻撃の緩和に使用されます。

3. **攻撃の緩和：**この段階では、いくつかの緩和方法から選択できます。疑わしい送信元にチャレンジを送信するために、最初の HTTPS 要求のトラフィック復号化を実行するように Radware DefensePro DDoS Mitigation を設定することを決定できます。また、SSL 証明書を使用できない場合は、疑わしい送信元からの HTTPS トラフィックの量をレート制限することで、攻撃を軽減できます。攻撃が完全に軽減されるまで、エスカレート方式で適用される複数の軽減方法を選択できます。

Radware ERT Active Attackers Feed

Radware ERT Active Attackers Feed は年間サブスクリプションとして利用可能で、Radware DefensePro DDoS Mitigation にプリエンプティブな保護レイヤを導入することで、Radware のお客様のアプリケーションとデータセンターの保護を強化します。

このフィードは、Radware DefensePro DDoS Mitigation に、最近 DDoS 攻撃に積極的に関与した攻撃者を高精度に示すリストのスプーフィングされていない IP アドレスを提供します。これにより、現在アクティブな既知の DDoS 攻撃者が自分の資産に近づき、攻撃を開始する前に、プラットフォームがプリエンプティブにブロックできるようになります。

Radware の ERT Threat Research Center では、既知のアクティブな攻撃者のリストを提供します。ERT Active Attackers Feed は、進化を続ける LoT ボットネットや新しい攻撃ベクトルなど、新たな DDoS 固有の脅威に対するプリエンプティブな保護を提供できる、独自のリアルタイム インテリジェンスに焦点を当てています。

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

ERT Active Attackers Feed のプロファイルは、ERT Active Attackers Feed サブスクリプションを利用して、以下を実行できます。

- Tor および Web 攻撃者のブロックを選択します。
- カテゴリとリスクレベル（[高（High）]、[中（Medium）]、[低（Low）]）ごとに [レポートのみ（Report Only）] モードを選択します。
- ポリシーごとに ERT Active Attackers Feed 保護を有効化および設定します。

トラフィック フィルタ

トラフィックフィルタは、Radware DefensePro DDoS Mitigation によるポリシーレベルでのトラフィック処理の制御を可能にする新しい保護機能です。トラフィックフィルタは、追加の手動制御により、Radware DefensePro DDoS Mitigation 保護を補完します。トラフィックフィルタを使用すると、指定した値と一致するトラフィック、または指定した値と一致しないトラフィックをブロックまたはレート制限できます。 また、ポリシー内の特定のネットワークアドレスまたはポート値をフィルタ基準として定義できます。

トラフィックフィルタの使用例は次のとおりです。

- **事前定義された最大レート：**保護されたネットワークおよびサーバーの最大レート（1 秒あたりのパケット数）を使用して、特定のポリシーに到達するすべてのトラフィックに対してトラフィックフィルタを設定できます。この事前定義されたトラフィックフィルタは、Radware DefensePro DDoS Mitigation から保護されたネットワークへの任意の時点での最大レートを制限できます。このようなフィルタは、
- Radware DefensePro DDoS Mitigation インスタンスの初期設定時に設定できます。
- **攻撃時のホワイトリスト登録：**保護されたネットワークに向かう Radware DefensePro DDoS Mitigation が検査するトラフィックのトラフィックフィルタを設定し、ポリシーに一致する可能性のある他のすべてのトラフィックをブロックできます。この方法では、予想される正規のトラフィックのみを検査し、このポリシーに到達する残りのトラフィックをブロックできます。これを実現するには、トラフィックフィルタで [不一致（Non-Matching）] オプションを指定します。
- **攻撃時のトラフィックのブロック：**ポリシーに到達する特定のトラフィックまたはすべてのトラフィックをブロックまたはレート制限するためのトラフィックフィルタを設定できます。

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

パケット異常保護の追加

新しいパケット異常保護：誤った GRE バージョン（ID 126）

この新しいパケット異常保護は、GRE バージョンが 0 または 1 ではないパケットを照合します。

新しいパケット異常保護：無効な GRE ヘッダー（ID 128）

この新しいパケット異常保護は、部分的またはスライスされたパケット、または 1 つ以上のフラグが RFC に準拠していないパケットを照合します。

シグネチャ保護アプリケーション セキュリティの機能強化

ERT Security Update Service（SUS）のサポート

Radware の Emergency Response Team（ERT）Security Update Service（SUS）は、ネットワーク要素、ホスト、およびアプリケーションを最新のセキュリティの脆弱性や脅威から保護するための、サブスクリプションベースのセキュリティアドバイザリおよびマネージドモニタリング/検出システムです。ERT は、サービス妨害（DoS）攻撃やマルウェアの発生に直面しているお客様に、年中無休のセキュリティサポートサービスを提供するセキュリティエキスパートのグループです。SUS は、シグネチャファイルの定期的な更新、影響の大きいセキュリティイベントへの迅速な対応、およびカスタムシグネチャの開発と配布を行うことで、現在のサブスクライバに迅速かつ継続的な更新を提供します。これらの更新は、選択に応じて、完全に自動化された方法または手動で実行できます。

ERT SUS は、次の主要なサービス要素で構成されています。

- **毎週の更新：**シグネチャファイルの定期的な更新をスケジュールし、通常は毎週、APSolute Vision による自動配信を行います。ERT SUS は、ほとんどの既知の攻撃ツールと Radware の ERT グループから直接送信された最近の脆弱性に対して保護を提供します。SUS の更新には、DoS フラッディングツール、低速 DoS 攻撃およびツール、DoS 単一パケットの脆弱性、および重要なデータセンター アプリケーションの脆弱性が含まれます。定期的な更新は通常、週単位で利用でき、以前に緊急更新としてリリースされたものを含むすべての新しいフィルタが含まれます。

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

- **緊急更新：**緊急対応が必要な場合、Radware は緊急シグネチャファイルのアップデートを発行します。緊急更新は、ERT 分析に基づいて、顧客を危険にさらす重大な脆弱性がある場合に、週次リリースとは別にリリースされます。これらの更新には ERT 脅威アラートが付随し、シグネチャの更新に加えて予防措置のガイダンスも提供します。緊急更新が Radware のドメインからダウンロードできるようになると、登録済みのお客様に電子メールで通知されます。

複雑なフィルタ

このバージョンの Radware DefensePro DDoS Mitigation では、アプリケーション セキュリティのシグニチャに複雑なフィルタを設定できます。複雑なフィルタは、同じシグニチャに割り当てられたフィルタのグループで、フィルタ間にブール AND 条件が存在します。この機能により、悪意のあるトラフィックの検索と照合の精度が向上します。

フィルタの追加コンテンツタイプ

このリリースの Radware DefensePro DDoS Mitigation では、アプリケーション セキュリティのシグネチャフィルタに多数の**コンテンツタイプ**のオプションが追加されています。オプションには、[HTTP要求ヘッダー（HTTP Request Header）]、[HTTP要求データ（HTTP Request Data）]、[HTTP URL]、[正規化されたHTTP URL（Normalized HTTP URL）]、および [HTTP Cookieヘッダー（HTTP Cookie Header）] が含まれます。

フィルタの追加コンテンツパラメータ

このバージョンの Radware DefensePro DDoS Mitigation では、アプリケーション セキュリティのシグニチャフィルタの設定に、追加のコンテンツパラメータが導入されています。追加のコンテンツパラメータには、[オフセットで検索を開始（Start Search at Offset）]、[オフセットで検索を停止（Stop Search at Offset）]、[一致するコンテンツ値（Content Value to Match）] があります。

シグニチャ保護アプリケーション セキュリティのシグニチャのための HTTP アクション

シグネチャ保護モジュールは、Web、メール、FTP、ワームやウイルス、トロイの木馬やバックドア、ボット、スパイウェアなどのサーバーベースの脆弱性から保護します。アプリケーション セキュリティ（AppSec）モジュールは、Radware Signatures データベースのシグニチャとユーザー定義のシグニチャを使用し、強力な文字列照合エンジン（SME）を採用しています。

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

このリリースの Radware DefensePro DDoS Mitigation では、アプリケーション セキュリティのシグニチャに対して次の追加アクションを設定できます。

- HTTP 200 OK
- HTTP 200 OK and Reset Destination
- HTTP 403 Req Forbidden
- HTTP 403 Forbidden and Reset Destination

SYN フラッド保護のための透過型プロキシ認証

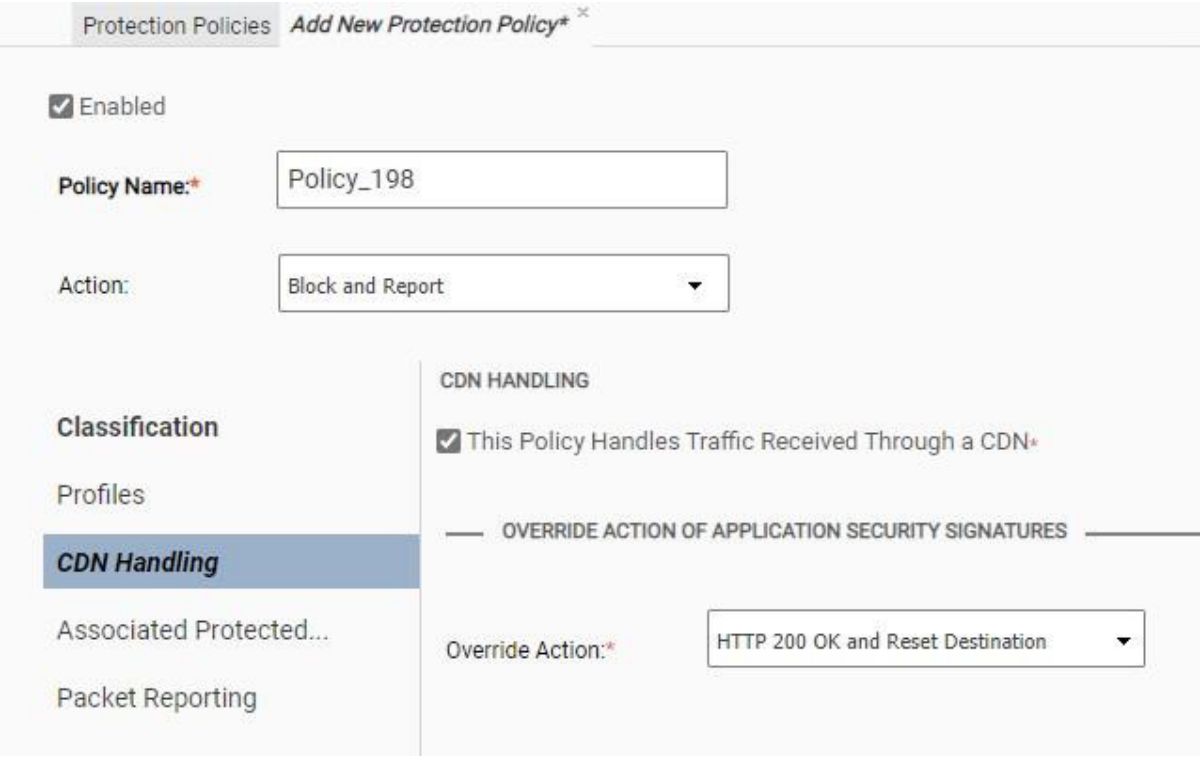
透過型プロキシは、SYN フラッド防御プロファイルの設定で使用できる追加の認証方式です。既存の認証方式である**セーフリセット**と **TCP リセットへの追加です。 透過型プロキシを使用すると**、Radware DefensePro DDoS Mitigation は SYN パケットを受信して最初にクライアントとの SYN Cookie を含む 3 ウェイハンドシェイクを完了することによって、TCP セッションを認証します。その後、セッションが正規のものであると判断されると、Radware DefensePro DDoS Mitigation は宛先との接続を開き、セッションの残りの間、送信元と宛先の間の透過的なプロキシとして機能します。

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

シグネチャ保護アプリケーション セキュリティによるポリシーごとの CDN サポート

このリリースでは、ポリシーによって処理されるトラフィックを CON から受信するかどうかと、受信する場合は、シグネチャ保護アプリケーション セキュリティのシグニチャが、シグネチャを照合するトラフィックに対して利用可能な HTTP アクションのいずれかを使用するかどうかを、ポリシーレベルで設定するオプションがあります。

図 4：CDN 処理ポリシーの設定



接続制限保護の一時停止アクション

このリリースの Radware DefensePro DDoS Mitigation では、接続制限保護に対する一時停止アクションのサポートが追加されています。設定に応じて、Radware DefensePro DDoS Mitigation は、接続制限攻撃の発信元である 1 つ以上の IP アドレスからのトラフィックを所定の期間にわたって一時停止できます。

さらに、繰り返し攻撃を行う送信元 IP アドレスを、一時停止時間を増やして何度も一時停止することができます。

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

古い未確立セッションの宛先のリセット

この構成設定により、Radware DefensePro DDoS Mitigation では TCP リセットパケットを古い未確立セッションの宛先に送信できるようになります。セッションが確立されていないか、または完全に確立されていないと DefensePro が見なすのは、[未確立セッションのエージング時間（Non-Established-Session Aging Time）] 内でセッションの確立が完了しない場合、

および [TCPハンドシェイク後にデータが送信された場合にのみセッションを確立済みとみなす（Consider Session Established Only If Data Sent after TCP Handshake）] パラメータの設定に従います。

大きな EDNS パケットを許可する

Extension Mechanisms Protocol for DNS（EDNS）は、DNS メッセージのサイズを拡張するための拡張メカニズムのセットです。最初の EDNS 規格は 1999 年に遡りますが、2019 年 2 月 1 日に、主要な DNS ソフトウェアおよびサービスプロバイダーが、ユーザーが EDNS をバイパスできるようにしていた DNS の回避策を削除しました。

現在、DNS プロトコルの準拠を確認する際に、大きな EDNS パケット（512 バイトを超えるパケット）を許可するかどうかを決定できるようになりました。

メッセージタイプ別の syslog 詳細レポートの有効化

Radware DefensePro DDoS Mitigation が設定された各 syslog サーバーに送信する syslog イベントメッセージのタイプを設定できるようになりました。設定するターゲット syslog サーバーごとに、Radware DefensePro DDoS Mitigation がセキュリティイベント、デバイス健全性イベント、および設定監査イベントを送信するかどうかを選択できます。

イベントタイプ別の SNMP トラップの送信の有効化

Radware DefensePro DDoS Mitigation が設定された各 SNMP ターゲットに送信する SNMP トラップメッセージのタイプを設定できるようになりました。設定する SNMP ターゲットサーバーごとに、DefensePro がセキュリティイベント トラップ、デバイス健全性イベントトラップ、および監査イベントトラップを送信するかどうかを選択できます。

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

TLS 1.3 および楕円曲線暗号化証明書のサポート

Radware DefensePro DDoS Mitigation のこのリリースでは、保護された SSL オブジェクトの設定の一部として、データトラフィックの TLS 1.3 暗号化プロトコルの設定と使用のサポートが追加されています。TLS 1.3 には、プライバシーとセキュリティの分野での大幅な改善が含まれており、その標準化時点（2018 年 8 月）で既知の脆弱性のないアルゴリズムのみがサポートされています。

また、このリリースでは、楕円曲線暗号化（ECC）証明書の使用サポートが導入されています。ECC は RSA よりも大幅に短いキーを使用するため、TLS ハンドシェイク中に検証されるデータが少なくなり、コンピューティング オーバーヘッドが少なくなります。

HTTPS 管理インターフェイスで使用される TLS バージョンを制御する CLI ベースのオプション

このリリースでは、CLI ベースのオプションである manage ssl version が導入されました。これにより、Radware DefensePro DDoS Mitigation の HTTPS 管理インターフェイスで使用される TLS バージョンを制御できます。

デバイス認証用 TACACS+

TACACS+ 認証サーバーを使用して、Radware DefensePro DDoS Mitigation にログインしているユーザーを認証できるようになりました。

ポリシーごとの CPU 使用率のモニタリング

共有デバイスの使用例を対象として、保護ポリシーごとの CPU 使用率をモニタリングすることで、Radware DefensePro DDoS Mitigation の各保護ポリシーによるリソース消費量を深く理解することができます。

可視性が追加されることで、次の場合に役立ちます。

- デバイスリソースの使用量を最適化するための保護ポリシーの調整
- 「消費量の多いコンシューマ」の検出
- 「ノイズの多い」保護ポリシーを調整、削除、または変更することによる、許容可能なデバイス CPU 使用率レベルの維持

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

保護ポリシーごとの CPU 使用率のモニタリングは、次の情報を提供します。

- APSolute Vision Analytics（AVA）AMS を使用したポリシーごとの平時および攻撃時の CPU 使用率グラフ
- ポリシーによる CPU 使用率アラートをアクティブ化および終了するための設定可能なしきい値
- AVA AMS、SNMP、および syslog アラートオプション

BDoS および SYN フラッド保護のプロファイル単位の詳細レポート設定

BDoS および SYN フラッド保護プロファイルでは、プロファイルに一致するトラフィックをブロックして報告するか、または報告のみを行うかを選択できます。

同時セッションのモニタリング用の SNMP 01D

次の 2 つの SNMP オブジェクト識別子（OID）が追加されました。

- OID.1.3.6.1.4.1.89.35.1.104.53：Radware DefensePro DDoS Mitigation デバイスによって監視されたセッションの総数を取得します。
- OID.1.3.6.1.4.1.89.35.1.104.54.1.2：Radware DefensePro DDoS Mitigation フローエンジン（OPE）ごとに監視されるセッション数を取得します。

変更内容

このセクションでは、バージョン 8.22.2.0 で変更された内容について説明します。

フラグメント化されたトラフィックに対する BDoS Real-Time Signature の最適化

BDoS Real-Time Signature（RTS）の作成中の frag-bit 属性の優先度を高くしました。この最適化の目的は、Radware DefensePro DDoS Mitigation BDoS モジュールによって、フラグメント化された攻撃の緩和を改善することです。

BDoS および DNS 保護のグローバル設定をプロファイル設定に移動

Radware DefensePro DDoS Mitigation のインスタンスごとにグローバルに設定できる、いくつかの BDoS および DNS フラッド保護設定が、プロファイルごとに設定できるようになりました。

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

設定は次のとおりです。

- BDoS フットプリントの厳格性
- BDoS ラーニング抑制しきい値
- BDoS オーバーブロッキング防止
- DNS フットプリントの厳密性
- DNS ラーニング抑制しきい値

DNS フラッド保護のグローバル設定

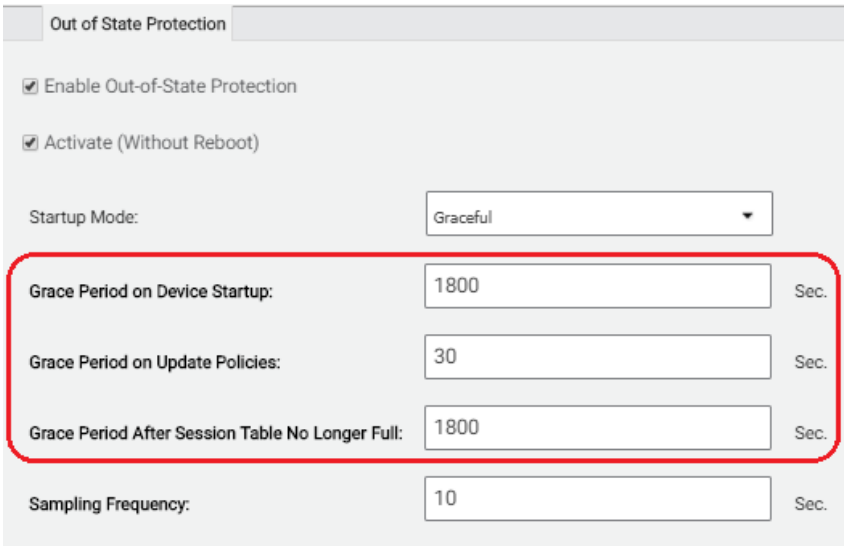
DNS フラッド保護がデフォルトで有効になりました。

Out-of-State Protection の猶予期間の設定オプション

Radware DefensePro DDoS Mitigation は、さまざまなシナリオに対応するために、Out-of-State Protection のアクションに対していくつかの異なる猶予期間を実装しています。これらの猶予期間中、Radware DefensePro DDoS Mitigation は、Out-of-State Protection の緩和アクションを遅延させます。

このリリースでは、APSolute Vision、CLI、および SOAP を使用したさまざまな Out-of-State Protection の猶予期間の設定オプションが導入されています。

図 5：Out of State Protection の猶予期間



© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

パケット異常保護の機能拡張：認識不能 L2 フォーマット（ID 100）

パケット異常保護の認識されない L2 フォーマット（ID 100）は、次のように拡張されています。

- 追加条件を追加
- デフォルトのアクションをレポートに変更

複数のパケットレポート宛先

パケットレポートの宛先として、最大 5 つの IP アドレスを設定できるようになりました。

NTP 設定

ユーザー設定の**ポーリング間隔**は、NTP サーバーが使用可能である場合、および NTP サーバーが到達不能または使用不可である場合に適用されます。

新しい CLIコマンドである services ntp server-last-poll が追加されました。このコマンドを使用すると、NTP サーバーの最後の正常なポーリングの時刻とNTPサーバー/デバイスの偏差を秒単位で表示できます。

SNMPv3 セキュリティのための 128 ビット暗号化

このバージョン以降、Radware DefensePro DDoS Mitigation は、128 ビットキーサイズの SNMPv3 での AES の使用をサポートします。AES-128 は SNMPv3 の暗号化機能を SNMPv3 標準を超えて拡張します。

SSH の強力な暗号化方式

このリリースの Radware DefensePro DDoS Mitigation では、デフォルトで、aes128-cbc、aes192-cbc、aes256-cbc などの強力な SSH 暗号化方式が有効になり、arcfour や blowfish-cbc などの弱いと見なされる SSH 暗号化方式がデフォルトで無効になります。

新しい CLI コマンドである manage ssh algorithm set を使用すると、SSH に使用する暗号化方式を設定できます。

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

ハッシュ化されたパスワードを使用しないファイル生成のサポート

デフォルトでは、DefensePro テクニカルサポートファイルを生成すると、そのファイルには常に暗号化またはハッシュ化されたパスワードが含まれます。

DefensePro がユーザークレデンシャルのないテクニカルサポートファイル（つまり、暗号化されたパスワードやハッシュされたパスワードも含まないファイル）を生成するように要求できる、新しい CLI コマンドが使用可能になりました。

コマンドの構文は次のとおりです。

system internal config-file remove credentials-info {011}

値は、次のとおりです。

- **0** は、機能が無効であることを指定します。つまり、生成されるテクニカルサポートファイルには、暗号化またはハッシュ化されたユーザークレデンシャルが含まれます。
- **1** は、機能が有効であることを指定します。つまり、生成されたテクニカルサポートファイルにはユーザークレデンシャルが含まれません。

デフォルト：0

その他の機能拡張

このバージョンの Radware DefensePro DDoS Mitigation には、その他にも次の機能拡張が含まれています。

- Radware DefensePro DDoS Mitigation デバイスパスワードが、ASCII の非アルファベット記号文字の使用をサポートするようになりました。
- ポリシー名の最大許容長が 64 文字に増加しました。
- Radware DefensePro DDoS Mitigation は、IPsecトラフィック、つまり IP プロトコル番号 50 および 51 を使用するトラフィックを常に処理します。
- syslog サーバーに送信されるメッセージでは、SNMP クレデンシャルがマスクされるようになりました。
- [診断ツールパラメータ（Diagnostic Tool Parameters）] の [キャプチャポートグループ（Capture Port Group）] パラメータのデフォルト値が、[データポート（On Data Ports）] になりました。

既知の制限事項

既知の制限事項のリストは、以下のリンクから入手できます。

https://support.radware.com/app/answers/answerview/aid/1025271

© 2020 Cisco | Radware. All rights reserved. This document is Cisco Public

関連資料

以下のドキュメントがこのバージョンに関連しています。

- *Radware DefensePro DDoS Mitigation 8.22.2.0 ユーザーガイド*

最新の Radware 製品ドキュメントについては、http:// portals.radware.com/Customer/Home/ を参照してください。