The NitroGuard IPS Engine, From the Creators of In-line Snort (IPS)

REPLACEMENT WHITEPAPER

230 Commerce Way, Suite 325, Portsmouth NH 03801 telephone: 603.766.8160 fax: 603.766.8169
nitrosecurity.com

Core Technical Competence

侵入検出と防止においてニトロセキュリティが革新を発展させて、セキュリティデータ管理は、約100人年の研究開発を、最初の荒い鼻息ベースのIPS、Snort_inline.1 Snort_inline〈v2.2の荒い鼻息に組み入れられた〉の作成を含むIPSテクノロジーに覆っている2000年以来、ニトロセキュリティによりさらに強化されて、強力で、カスタムの侵入検出と防止エンジンを作成するために、荒い鼻息から向こうに分岐していました：ニトロガード。

ニトロガードは、設定されて、脆弱性研究においてニトロセキュリティ脅威分析センター（NTAC）から基づくカスタムのサインを使って強力なIPSエンジンです。ニトロガードが荒い鼻息によってサイン互換性を維持する間、ニトロガードは、最高250%の性能増加を含む荒い鼻息より多くの利点を提供します。従って、4,500を超えるcustombuilt規則の新しいサインセットが提供されて、ニトロガードIPSエンジンを完全に利用します。同時に、ニトロガードが荒い鼻息シンタックスと互換なので、ニトロガードは容易にカスタマイズ可能で、拡張可能です。

ニトロガードIPSエンジンのいくつかの具体的な機能が含みます：

1. パケットブロックと部分修正を持つ高性能インライン検出（IPSモード）
2. IPv6ネットワークでのIPv6サポート、可能化IDS、およびIPS。
3. プロフィール柔軟性とサイン性能のために同時のSnort_Inlineエンジン（「バーチャルなIPS」）のためにサポートしてください。
4. イベント／フロー相互関係および流れベースのセキュリティサインでの使用のために、フローコレクションをネットワーク化してください。
5. 規則前処理、サイン処理、および性能の改良。
6. 間違いのポジティブと増加パケットスループットをかなり減らすニトロガードIPSエンジンのための進行中のサイン開発。

これらは以下の利点を結果として生じます：

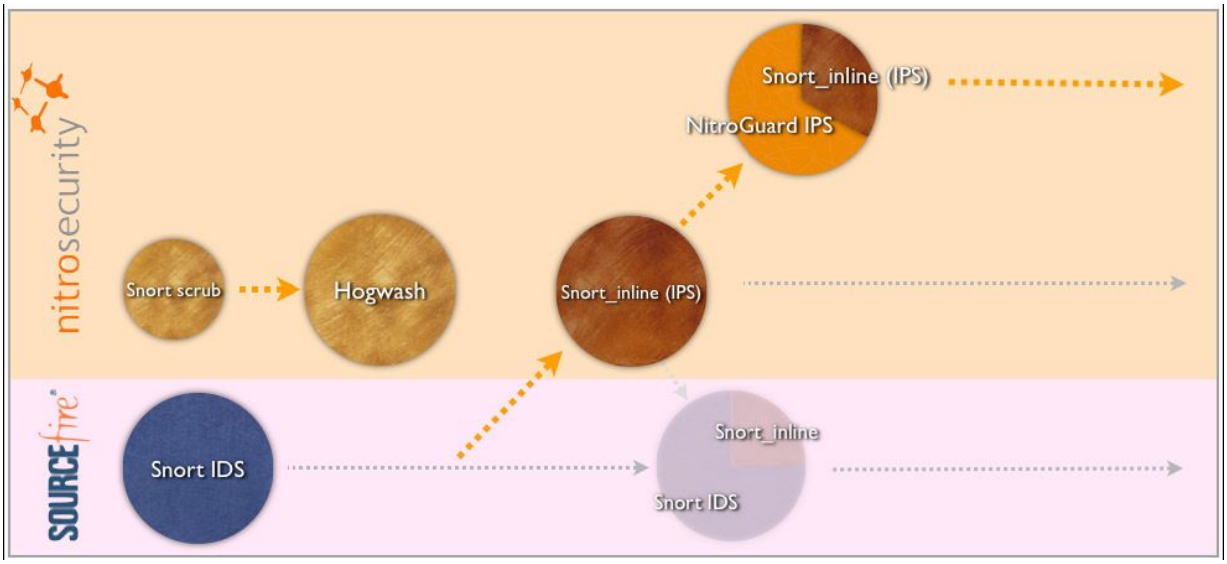
1. より少ないサイン、下の潜在性、およびより高いスループットによってより多くの脅迫を妨げる能力。
2. 0日攻撃を含む新しい脅威を適応させるサイン柔軟性。
3. 間違いのポジティブの重要な縮小。
4. その上において規則が使われる where、およびby whom 単一のニトロガードIPSがもっと遂行することを可能にする 方針ベースのコントロール。

これらの開発の多くは、IPS、SIEM、NBA、およびログ管理の機能と機能が単一で、高く統合されたシステムに集中する一体化セキュリティマネジメントのニトロセキュリティのビジョンの実現を表しています。

1 最初の荒い鼻息ベースのIPSは、2000年にニトロセキュリティエンジニアジェイソンラルセンにより開発されたプロジェクトでした。プロジェクトはもとは「荒い鼻息低木」と呼ばれました。それは、より遅い新しく名前をつけられた残飯でした。残飯はDEFCON 2001で2001年に公表されました。Snort_Inline〈技術的に2番目のsnortbasedされるIPS〉は、2002年に開発者ジェドHaileによってニトロセキュリティにより作成されました。Snort_InlineはHoneyNetプロジェクトに与えられました。HoneyNetプロジェクト〈もとはSun Microsystemsの強奪McMillenとランスSpitznerにより維持された〉は、荒い鼻息と別です。

IDSとIPSの開発歴史

侵入検出はしばらくあったけれども、荒い鼻息、標準のシンタックスにおいて書かれたサインに対して交通を比較するオープンソーステクノロジーの導入によって広く使われました。荒い鼻息サインシンタックスは、セキュリティプロフェッショナルによって広く理解されました; 荒い鼻息が自由で(オープンソースライセンスの下で配布されます)ので、それはなり 広く使われるおよび 、現在効果的に事実上のIDS標準です。それが、検出するようにデザインされたので、荒い鼻息がIDSテクノロジーであるけれども、侵入を防止しないために: ネットワークパケットのコピーに制限されているトラフィックで分析します。これのため、もし脅威が発見されたならば、行動を取りやすい方法が全然ありませんでした。むしろ、荒い鼻息が検出したことおよび脅威の、警報を出されたセキュリティプロフェッショナル: すなわち、侵入検出システム、またはIDS。



荒い鼻息での次の革新 パケットを落とし、荒い鼻息と別に、同じおなじみのサインシンタックスを使って始めたか、または修正する能力によってライブのネットワークトラフィックに荒い鼻息を通過させる能力 。荒い鼻息IDSをIPSに効果的に変えるこの革新は、最初、早い2000年に、後で残飯に新しく名前をつけられた荒い鼻息低木と呼ばれるプロジェクトによってニトロセキュリティのジェイソンラーソンにより試みられました。その後すぐ、ジェドHaile(ニトロセキュリティのまた)は、現在Snort_Inlineとして知られているもののオリジナルのバージョンを開発しました(もとは、ip_queueに基づきました)。2 ジェドのオリジナルのSnort_Inline仕事は、また、後ろに荒い鼻息(荒い鼻息バージョン2.3.0RC1の)に受け入れられて、荒い鼻息バージョン2.8.x現在まだ入手可能です。リアルタイムのライブの交通によって働くSnort_Inlineの能力は、TCP/UDP部分修正によってインライン検査を許します。すなわち、パケットは、検査されたインラインおよび直ちに代行すること 時 です(セッションを含み、リセットします 落ちているパケット、および他のより攻撃的な行動)。Snort_Inlineが荒い鼻息に基づくので、既存の荒い鼻息IDSサインは侵入防止のために使われえました。Snort_Inlineは、広く採用されました: 最初の本当の荒い鼻息ベースのインライン侵入防止システム、またはIPSは、ニトロセキュリティにより作成されました。これらの最初から、より一層の研究開発は別の主要なセキュリティ革新を引き起こしていました: ニトロガード侵入防止エンジン。

2 Snort_Inline開発者は以下でリストされます: http://sourceforge.net/project/memberlist.php?group_id=78497と包括デイブ再物腰(ニトロセキュリティ)。Snort_Inlineは、作成を、Snort_Inline配布

(http://sourceforge.net/project/showfiles.php?group_id=78497)において文書化されたジェドHaile(ニトロセキュリティ)に帰しています

Snort_Inlineの早いバージョンは、バージョン2.3.0RC1 Snort_Inline名前を保持し、現在の管理者／開発者と同様に著作権所有権をジェドHaile（ニトロセキュリティ）と強奪McMillenに帰している の荒い鼻息に寄与されていました：ウィリアムメトカーフ、ビクタージュリアン、ニックRogness、およびデイブ再物腰（ニトロセキュリティ）。3

Snort_Inlineの開発はかなり進歩したけれども、SourceFireにより管理されるような荒い鼻息の主要な開発枝は、荒い鼻息に少しのSnort_Inlineパッチを受け入れて、バグ修正はバックするだけです。 Snort_inlineは荒い鼻息から別々に進化し続けて、荒い鼻息に含められているようにSnort_inlineのバージョンの上のいくつかの主要な革新を含みます。 ニトロガードは、次々、多くの進歩が後ろにopensourceライセンスの心の荒い鼻息インラインコミュニティに提供されるけれども、Snort_inlineから別々に進化し続けます。

ニトロガードIPSは、今日入手可能な最も強力なおよび柔軟なIPSシステムのうちの1つを表しています。 IDAまたはIPS器具で以前に利用できなかった荒い鼻息サインシンタックスを持つ後ろ互換性の組み合わせ、ニトロセキュリティNTACからの微調整されたサインの新しいカスタムのセット、および新しい機能と機能。 ニトロガードで入手可能な重要な機能と向上は含みます：

＊統合されたネットワークフロー自覚

＊相互関係とポスト処理のためのイベントとフローデータの、統合されて、高速なストレージ

＊最高250%の性能増加を結果として生じる中心的なテクノロジー向上

＊ユニークなサインセットと方針を持つそれぞれというバーチャルなIPS操作（複数のSnort_Inline例）

＊頑強なIPv6サポート、改善されたHTTP前処理、および荒い鼻息の上の他の中心的な改良

3 バージョン2.3.0RC1〈ここでhttp://www.Snort.org/dl/old/Snort-2.3.0RC1.tar.gzを配布する〉のための荒い鼻息リリース・ノートは、これらの寄与を認めます。 また、それが言及されるべきである that 強奪McMillen 、ウィリアムメトカーフ、ビクタージュリアン、およびニックRognessは、Snort_Inline著作権についてのさらに無効化SourceFireの主張というSourceFireを表していません。

NitroGuard Innovations

ニトロガードは、ニトロセキュリティ(最初の荒い鼻息ベースのIPSの創造者)からセキュリティ専門知識の結果であり、荒い鼻息ベースの侵入防止の外の多くの革新だけでなく荒い鼻息サイン処理という荒い鼻息およびSnort_Inline(IPSモード)においていくつかの革新を表しています。これらは、ニトロガードおよび「統合されたセキュリティマネジメント。」の会社のビジョンを実現するように特にデザインされる他のニトロセキュリティ製品内の機能の開発を含みます。

これらの開発の多くは下で強調されて、以下のカテゴリーに分割されます:

＊革新を吹き出してください(後ろに基本の荒い鼻息配布に組み込まれた寄与を吹き出してください)。

＊Snort_Inline革新(後ろに基本のSnort_Inline配布に組み込まれたSnort_Inline寄与)。

＊追加の荒い鼻息&Snort_Inline革新(後ろに基本の配布に実施されなかった寄与)。

＊他のニトロガード革新(荒い鼻息とSnort_Inlineの外の革新)。

Other NitroGuard Innovations

ニトロセキュリティのニトロガードIPSエンジンが、SourceFireにより管理されるように基本の荒い鼻息配布で造られていると考えられない間、2回の非常に重要な開発が、荒い鼻息に寄与されていました。これらは、オープンソース 荒い鼻息プロジェクト において、ニトロセキュリティに与えられた著作権所有権によって含有のためのSourceFireに提供されて 荒い鼻息コードベースの中に 、受け入れられました。4

＊サインマッチが起こる時には、インライン／IPSモードイニシャルインラインサポート(ip_queueはIPSの基礎に相当していました)、ニトロセキュリティが発展すること、および導入されることが、行動が取られることを可能にします。なぜなら、個々の規則は、コピーされた交通というよりもライブの交通(インライン)に対して実行されるからです(不インライン、またはIDS)。これは、検出されるだけであるというよりも攻撃が防止されることを可能にして、パケットがリアルタイムに落とされることを可能にします。

＊パケットマニピュレーションパケットマニピュレーション機能〈ニトロセキュリティにより導入された〉はパケットのリアルタイムの変更を可能にします。

Snort_Inlineの統合に先がけて、荒い鼻息は検出単の(IDS)テクノロジーでした。インライン、最初の荒い鼻息基づいたIPSがニトロセキュリティに信用される起訴可能な荒い鼻息の統合。5

4 GPLv2の条件ですべての革新が提供される間、多くの革新は具体的な環境(ニトロガードIPSなどの)と関連するだけで、従って、主要な荒い鼻息配布において含有のために考慮されません。

これはSourceFireの自由にあります。その人は現在荒い鼻息GPLを管理します。

5 Snort_Inlineの起源の前の引用に加えて、Snort_Inline統合への確認は、http:// www.Snort.org／dl／古さ／荒い鼻息-2.3.0RC1.tar.gzで入手可能に、SourceFireの荒い鼻息リリース・ノート〈v2.3.0RC1の配布に含められている〉内で提供されます。

Snort_Inline Innovations

Snort_Inlineは、Honeynetプロジェクトの一部として荒い鼻息から別々に維持されるオープンソースプロジェクト〈それ自身の右の〉です。Snort_Inlineがオープンソースであり、GPL2の下にライセンスされるので、それは私達のニトロセキュリティ製品での使用で自由に利用可能です。そこで存在するので、Snort_Inlineが別個のプロジェクトとして発展し続ける ユーザーのコミュニティは、たとえSourceFireが、そうしないことを選んでもSnort_InlineがSourceFireの荒い鼻息に追加する機能と機能を維持し、強化する時に興味をもたせました。1つのそのような向上は、ip_queueの代わりに、IPSモード操作を大幅に改善してLinux netfilterに部分修正を使います： それは、よりよいIP処理、より大きい性能、および効率を考慮しました。

ニトロセキュリティに信用された具体的なSnort_Inline革新は含みます：

＊**Multi-Snort** –具体的 それによってSnort_Inlineの複数の同時の例を動かす能力ユーザー定義された場周経路のためのコンフィギュレーション（定規はセットします）を吹き出してください。また、「バーチャルIPS。」として知られています。

＊**IPv6**–ニトロセキュリティは、ケンルナールのオリジナルのIPv6荒い鼻息コードをSnort_Inline、および加算重要向上に移植するために、ビクタージュリアンに出資しました。これらの向上は、トンネルを掘られたIPv4とIPv6交通のICMP6とDHCP6、および提供検査をデコードすることを含みます

「マルチIPS」向上は、荒い鼻息のSourceFireの配布に含められているSnort_Inlineのより古いバージョン内でサポートされないSnort_Inlineへの重要な寄与です。この機能は、共通の機器内で、個々のバーチャルなIPSにおいて具体的なコンフィギュレーションをサポートする能力によって動くように、IPSの複数のバーチャルな例を可能にします。これは、物質的なIPSインタフェース、またはバーチャルなインタフェース（VLAN）に強制される具体的な役割ベースのコンフィギュレーションを考慮します。さらに、これは荒い鼻息シンタックス分析のスケーラブルな実施を可能にします： すなわち、もし特に複雑な規則がプロセッササイクルを消費しているならば、ニトロガードIPSは定期船を「守り」、IPSの他のバーチャルな例がトラフィックを調査し、より複雑なプロセスが完成されている間規則を実施し続けることによるスループットを制限しません。これは、ハードウェアベースの荒い鼻息加速の必要なしでのIPS性能のプロセッサ縮尺を可能にします（ハードウェア加速は理論上サポートされて それ 、この時ニトロガード内で使われないけれども、）。1.5Gbps（低い潜在性による）のレートのニトロガードのラインレートスループットは、主としてマルチIPSの性能利点のため現在サポートされます , IPSモード（または「ブロック」 モード ）。

Additional Snort and Snort_Inline Innovations

さらに、 鼻を鳴らし、Snort_Inlineが後ろにコミュニティに寄与されていたけれども、ではなかった 実施したニトロセキュリティの向上の多く ,去り唯一の所有権 知的所有権 ニトロセキュリティ 。

これらの革新は含みます：

＊**Home Net fix** –ほめられたアドレスによって家庭のネットを定義する能力：

今日壊されると考えられる荒い鼻息のエリア。

＊**Signature Innovations** –いっそう遠くに性能を改善するために、ニトロセキュリティのサインライブラリは精神のIPS機能によって最初から発展しました。標準が鼻を鳴らすことは決定されました。

ライブラリ（荒い鼻息によって配布されます）は、単一の功績に対して防御するために、時々数ダース、または均一な数百のユニークなサインを用いるので、しばしばIPS操作に不適当でした。弱点と功績、および標準の荒い鼻息シンタックスを慎重に調査することによって、私達はすることができます：IDSユーザーと対比されるようなIPSユーザーのニーズへの曲サイン；ニトロガードのユニークな機能と機能を利用してください；ニトロガードのスループットを最大化してください；そして、ニトロガードにより顧客のネットワークに提供された保護を最適化してください。結果として、功績の同じ数は、サインのアクティブな数の半分をおおよそ使って防止できました。これは以下の第2の利点を結果として生じます：

＊**Signature Performance** –サイン性能Aより小形サインベースは保護を捧げずに少ない処理、改善性能を必要とします。注：マルチSnort_Inline操作は、複数の平行したSnort_Inline操作を許してサイン性能をさらに改善します。

＊**Signature Tuning** –より小さいサインベースは、個々の個々のサインに使われるより大きい時間と努力を可能にします。IPSがより複雑に省略することを可能にし、例えば、容易に処理されるサインのそれらの部分はであるかもしれず もしもうそれらの部分が必要ではないとの決定プロセッサ集中的部分 、最初にチェックしました。

＊**Manageability** – それらがニトロガードにあるより特にグループと方針のためサインが扱いやすい時には、より少ないサインは管理しやすい。

＊ネットワークを完全に保護するために4,000未満のサイン（4,600+総規則の）のデフォルト規則セットが利用できることが、これらのサイン凝った工夫のためであり、逃されたまたは失われたパケットなしで100%インライン（IPS　モード）を操作します。

＊**Additional changes** – ニトロガードカスタム機能をサポートするために必要であったオリジナルの荒い鼻息コードベースの約15%と等　しい追加の部分修正。例えば：

＊荒い鼻息がNitroEDB関係データ管理エンジンに出力することを可能にするアウトプットplugins。

Other NitroGuard Innovations

多くの革新は、荒い鼻息またはSnort_Inlineに関係しないニトロガードIPSの開発にわたってされました。これらの開発は、Linuxカーネル（いくつかが専有的で、いくつかがGPLです）の部分修正および／または特許を取得したニトロセキュリティデータベーステクノロジーのインプリメンテーションに関係します。彼らが荒い鼻息とSnort_Inlineをほめる間、これらの革新の多くは、閉じられるライセンスの下のニトロセキュリティにより完全に所有されます。

これらの開発の多くは、IPS、SIEM、NBA、およびログ管理の機能と機能が単一で、高く統合されたシステムに集中する一体化情報セキュリティのニトロセキュリティのビジョンの進行中の実現を表しています。このビジョンは少しの主要な違いによってSourceFireの「3D」システムと比較できました：ニトロセキュリティのかなりの知的所有権包囲データ分析は、共通のデータ店、およびリアルタイムにおいて、私達が、すべての統合された機能を一緒に実行することを可能にします；追加の知的所有権は、行動または情勢分析のための後処理データに必要を取り除き、データが収集されると代わりにリアルタイムにおいてこれらの仕事を実行することによって、私達が分析的な計算を実行すること「飛行中で」を可能にします。ニトロセキュリティはこれらでユニークです。

約300人年の研究開発を表している特許を取得したテクノロジーのためニトロセキュリティ製品スイート内で可能であるだけの機能。

＊**Reassembly Improvements** –それをstream4／reasemblyに処理することへのアップデートは、パケット再アセンブリを取り囲んでいる重要なバグ修正について責任があります。

＊**HTTP Pre-processor Improvements** –100%はHTTPプリプロセッサで書き換えます。それは間違いのポジティブの重要な縮小を結果として生じました。荒い鼻息内のHTTP前処理は、警告の信頼性の欠如のため、今日、多くで、『壊されます』と考えられます。

＊**NitroEDB** – ニトロセキュリティの特許を取得したデータベースは、個々のニトロガードIPS機器においてレコードがキャッシュされて、圧縮されることを可能にします。NitroEDB（それから、ニトロガード）がイベントを挿入できるスピードは、侵入を検出し、防止する能力に影響せずにキャッシュしているイベントとフローを許します。さらに、丸いキャッシュメカニズムは、過度なロードの間の標準の荒い鼻息システムおよび／または導かれたサービス拒否攻撃に影響するかもしれない使用、防止キャッシュオーバフローです。

＊歴史のパースペクティブをIPSなどのインライン機器に維持する能力は、1秒あたり50,000の新しいイベントを受け取るいつでさえ、数ミリ秒で10億を超えるレコードについて情報を検索する可能性があるニトロセキュリティのデータ管理エンジン（NitroEDB）の生の性能のため可能であるだけです。

＊典型的な展開、月、または均一な年のフローに、イベントおよび用心深いデータは、ニトロガード機器自身内で格納できます。ニトロガードからのニトロ眺めへのデータの転送が中断されている時には、これの価値はいくらかの理由のために来ます。このシナリオに、通信割込みが解決される時には、ニトロガードは、他のIPS機器と違って後の方の検索のために、そのデータを蓄えます。さらに、ストレージ配列する 、および時間 フロー、イベント、および用心深いデータの検索 は、高可用性／冗長なアーキテクチャ内の複数のニトロ眺め器具の使用を自動的にサポートします。

＊**Blacklisting** –正常なIPS行動（警告、ブロック、リセット、パスなど）に加えて、規則基礎による規則では、ニトロガードは、時間の指定された量内の具体的な規則指定の数時を引き起こすソースIPからすべての交通を落とすことができます、そして、時間の別の指定された量の後に、ソースIPからこの落下行動を取り除いてください。

＊例：もしサインマッチが功績を検出するならば、時間のある量のためのソースIPから来るALL交通を妨げてください。または恒久的に。

＊**Flow Collection and Caching** –ニトロガードは、部分修正を、それがフロー情報を収集することを可能にするLinuxカーネルに持っています。この情報は、開始時刻、終わりの時間、および双方向のパケットとバイト計算を含みます。

＊**Invisible IPS operation / “Stealth Mode”**– IPアドレスなしでニトロ安全装置IPSが動作する能力。それが調査または発見プロトコルによって発見できず、それから、それほど、IPS自身が、切り刻まれることに陥りやすくないように。

＊**Integration with NitroView**–ニトロセキュリティの一体化セキュリティマネジメント(USM)ビジョンは、ニトロ眺めのコレクション、ユニフィケーション、および分析機能に依存しています。SourceFireの「3D」ソリューションのように、ニトロセキュリティは、独立して動作するかもしれないけれども、一緒に使われる時に強化される無料の製品を提供します。ニトロ眺めは、リアルタイムのネットワーク分析、ログ分析、およびセキュリティイベント分析の統合を分析のための共通のシステムに含み、報告しているいくつかのエリアのSourceFireのソリューションより役に立ちます。ニトロ眺めは、また、ニトロ眺め向上がニトロガードの操作を特に改善するポイント、および逆もまた同様にニトロガードIPSと高く統合されます。

＊**Post-Analysis Remediation / Blacklisting** –ニトロガードのブラックリストへの記載はaにより設定されます。ニトロ眺めのかなりの分析的な機能、および広大な量の格納されたデータを使って手に入れられた情報に呼応して規則によって規則基礎、普段においてニトロでユーザーを見てください。他の改善方法(それ IPS を必要としない)は、その上使われえます。

＊**IPS Group/Policy Management** –ニトロ眺めは、階層的な方針管理システムが、ユーザーがニトロガード機器を正しく容易に設定することを可能にすると規定します。

＊**Correlation of Logs, Event Data, and Network Flows** –ニトロセキュリティはNitroEDBデータです。管理テクノロジーは、広大なデータ量を迅速に蓄えて、分析することができます。この機能は、ニトロ眺めユーザーに、ユニークな能力 イベントを急速に関係づけている, を提供し 何が起こるかを知っている警告、フロー、およびログデータ か、またはそれらのネットワークで起こりました。

＊**Visual alert-to-endpoint mapping** –ニトロ眺めは完全なネットワークインフラストラクチャー、および終点発見をサポートします。それは、フロー、イベント、および用心深い情報が直接視覚化するアクティブなトポロジー眺めを築くために使用されます。このネットワーク&イベント分析トポロジー(清楚)は、ネットワーク化およびイベント変則の場合–a–一見インジケータを提供します。

Industry Recognition

Common Criteria Evaluation

ニトロガードは、EAL27をもたらしたSourceFire IPSと対比されるように共通標準EAL36を得ました。EAL 2とEAL 3の違いはテスト方法に関係します: EAL 2「構造上テストします」機器 間 EAL3「整然と、テストし、チェックします」機器 。すなわち、EAL3証明は、意図されているように、性能と機能主張をバックアップする整然としたテストデータによってそのニトロガードIPS機能を有効にします。

SC Magazine "Recommended" Product

ニトロガードIPSは、上層土、IBM-ISS、反射、CounterSnipe、および他に対する直接的な比較テストにおいて、「推奨されます」IPS製品として選ばれました。テストにより、機能、性能、使いやすさ、およびサポートのニトロガードIPS 5スターが授与されました。IPS〈広いラボテストに基礎を置く〉のこの公平な評価は、ニトロガードが、IBM-ISSなどの製品の上のより優れた保護を提供するのを見せて、ニトロセキュリティのNTACの経験が、非常に競合するサインセットを提供することを証明します。テストにより、ハードウェア加速されたIPSシステムによって同等を演奏すると、最大の柔軟性のためにソフトウェアベースの非常に調整されたニトロガードIPSエンジンも示されます。

SC Magazine "Innovator, 2007" Product

IPSが発展し、より大きいシステムの1つの部分になります。ニトロ見方企業保障マネジャー〈統合されたセキュリティマネジメント器具〉のニトロセキュリティの開発は、これを表しています。ニトロガードとニトロ眺め機能の私達の統合により、SC雑誌「革新者」賞は、2007 それゆえ「IPS、ESMおよびレシーバーすべては、事のためにその高性能系図のため他のシステムを全然することができなかったシステムに発展しています することができた 。」にもたらされました。

6 http://www.niap-ccevs.org/cc%2Dscheme/st/?vid=10132

7 http://www.niap-ccevs.org/cc-scheme/st/index.cfm/vid/4017

8 評価証拠の評価チームのアセスメントは、STでの主張が迎えられるのを証明します。

さらに、ベンダテストスイート、独立なテスト、および貫通力テストの全体の評価チームの性能は、ST.での主張の精度も示します「共通の標準評価および認証計画認証リポートから、http://www.niap-ccevs.org/cc-scheme/st/st_vid10132-vr.pdf

NitroGuard Today

ニトロセキュリティはであり、侵入防止システムの革新のインストルメンタル、およびネットワークセキュリティ情報収集と分析であることを続けます。これのため、今日それが存在するので、ニトロでガードしてください 費用効果が高く、容易に維持されたネットワーク器具の多くの高度な機能を提供する：

＊アップのサポートされたスループット 最高12の物質的なギガビットインタフェースにそれを持つ1.5Gbps 。スループットは、功績を塞ぐようにデザインされたIPSサインセットを使う間監視されて、妨げられうる交通の支えられたレートを参照します。（注：ニトロガードIPSの調整により性能は改善できる一方、一定のネットワーク環境変数は性能を低下できます。従って、寸法決め分析はIPS設備に先がけていつも実行されるべきです。ニトロガードIPS機器は、実世界の予想）を反映する共通のネットワーク環境および効果的なサインベースのために評価されます。

＊入手可能な物質的なインタフェースを横切る最高8つのバーチャルな例、または4,095のVLANsの完全な範囲に含むバーチャルなIPS例のサポート。バーチャルなIPS操作は全体の性能を低下させず、管理されたb方針であるかもしれず、個々のバーチャルなIPSが、彼らが監視する物質的またはバーチャルネットワークに特有なユニークな規則セットを強制することを可能にします。

＊約4,600のサインから成る非常に効果的なサインベースのためにサポートしてください。この高く調整されたサインベースは、標準の荒い鼻息サインセットといくつかの点で違います：

・ニトロガードの改善されたサインデザイン〈操作を簡素化し、性能を改善する〉のため、より少ないサインは、弱点と功績の同じ数に対して保護するために必要です。

・上で述べられているので、すべてのサインはアクティブな検出とブロックのために使われえます。適切に大きさで分けられたニトロガードモデルを使う時に、IPSモードにおいて動作する時に、刑罰が全然ありません。

＊間違いのポジティブなイベントと警告の重要な縮小 HTTPベースのサインで特に 。

＊荒い鼻息規則エディタの統合 ニトロガードの管理インタフェース内で規則が作成されて、編集されることを可能にする 。このエディタは切断&を含みます bleedingSnort.comなどのソースからの荒い鼻息サインの容易な付加のペーストサポート 。

＊フロー情報収集のサポートは、ニトロガードの統合されたフローコレクター、およびニトログリセリンRecevierのnetFlowとsFlowコレクション機能を使ってより頑強なサインを考慮します。

＊ユーザ定義の通知書と服従リポートのサポートを報告します。