Stealthwatch の段階的アプローチによる調整

最終更新日：2019 年 11 月 7 日

このガイドを使用して、Stealthwatch Enterprise v7.1 を調整するためのシンプルな段階的アプローチを学習できます。このガイドは、正式な Stealthwatch トレーニングに代わるものではありませんが、調整フレームワークを使用して Stealthwatch の運用を簡素化するフレームワークの実現に役立ちます。フローエクスポータの新しい集合が展開に追加されたときに、これらの手順を繰り返します。

アラームの解釈に関する追加情報については、以下を参照してください。
https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/securit_events_alarm_categories/SW_7_1_Security_Events_and_Alarm_Categories_DV_1_0.pdf [英語]

対象読者

このガイドは、Stealthwatch、ホストグループ、およびポリシー管理の基本的な知識を持つユーザを対象としています。用語の参照情報については、『SMC Users Guide』およびオンラインヘルプを参照してください。
https://www.cisco.com/c/dam/en/us/td/docs/security/stealthwatch/management_console/smc_users_guide/SW_7_0_SMC_Users_Guide_DV_1_1.pdf [英語]

トレーニング内容

利用可能なトレーニング内容のリスト：
https://www.cisco.com/c/en/us/products/security/stealthwatch/learning-services.html [英語]

6 段階のアプローチによる調整

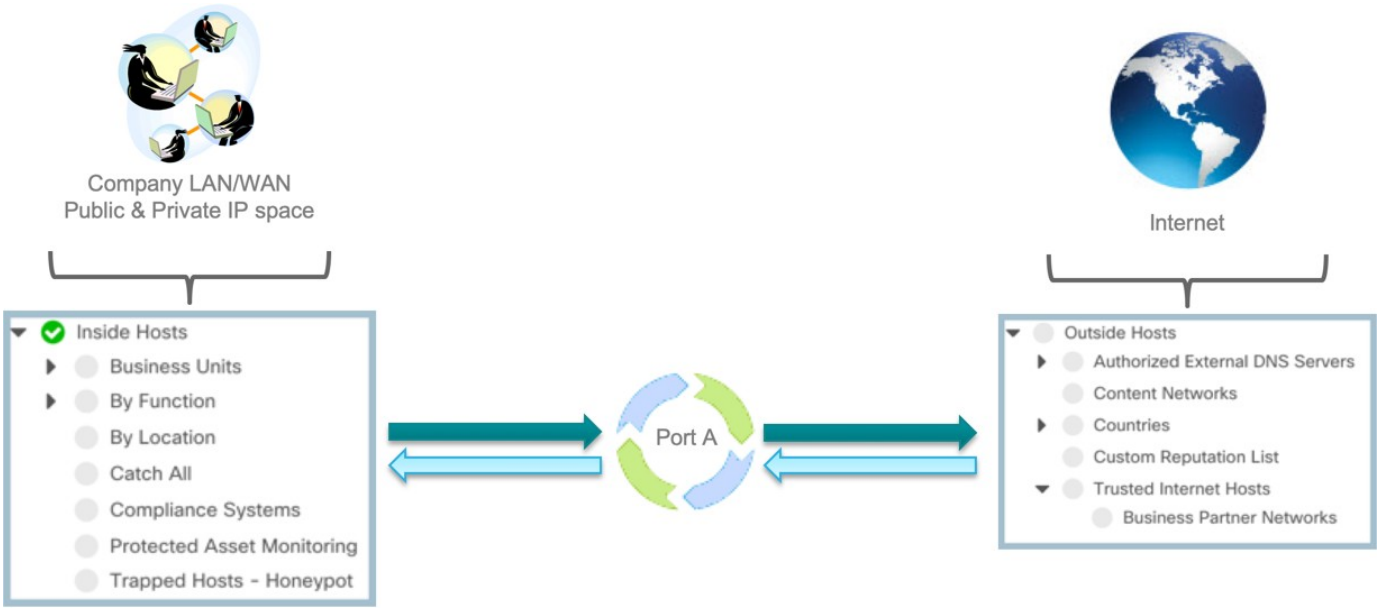
Stealthwatch では、機械学習を適用するだけではなく、ビジネスロジックとポリシーを柔軟に適用して脅威を検出できます。この目的は、きめ細かな分類、ホストグループ、カスタム セキュリティ イベント、およびカスタムポリシーをビジネスニーズに合わせて適用できるようにすることで実現されます。

フェーズ 1：内部の分類

RFC1918 とパブリック IP を内部に導入する

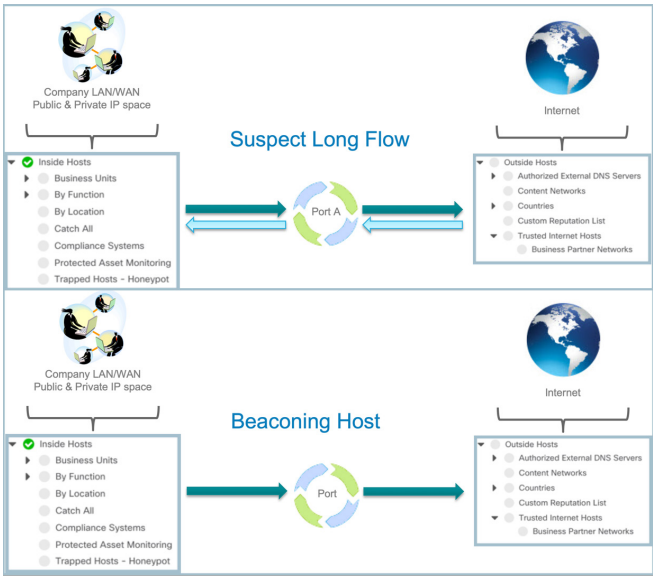
デフォルトでは、LAN/WAN インフラストラクチャまたは「内部ホスト」を構成するものを定義するまで、すべての IP アドレス空間は外部ホストグループに属しています。

インターネット（「外部ホスト」と呼ばれる）を内部ホストから分離すると、インターネットとの間で送受信される疑わしいトラフィックを検出できるようになります。



内部ホストグループを分類することが重要である理由

内部トラフィックと外部トラフィックの間に焦点を合わせてトリガーされるアラームがいくつかあります。組織が所有する IP スペースをキャプチャすると、誤検出が減少します。



影響を受けるアラームには次のアラームが含まれます。

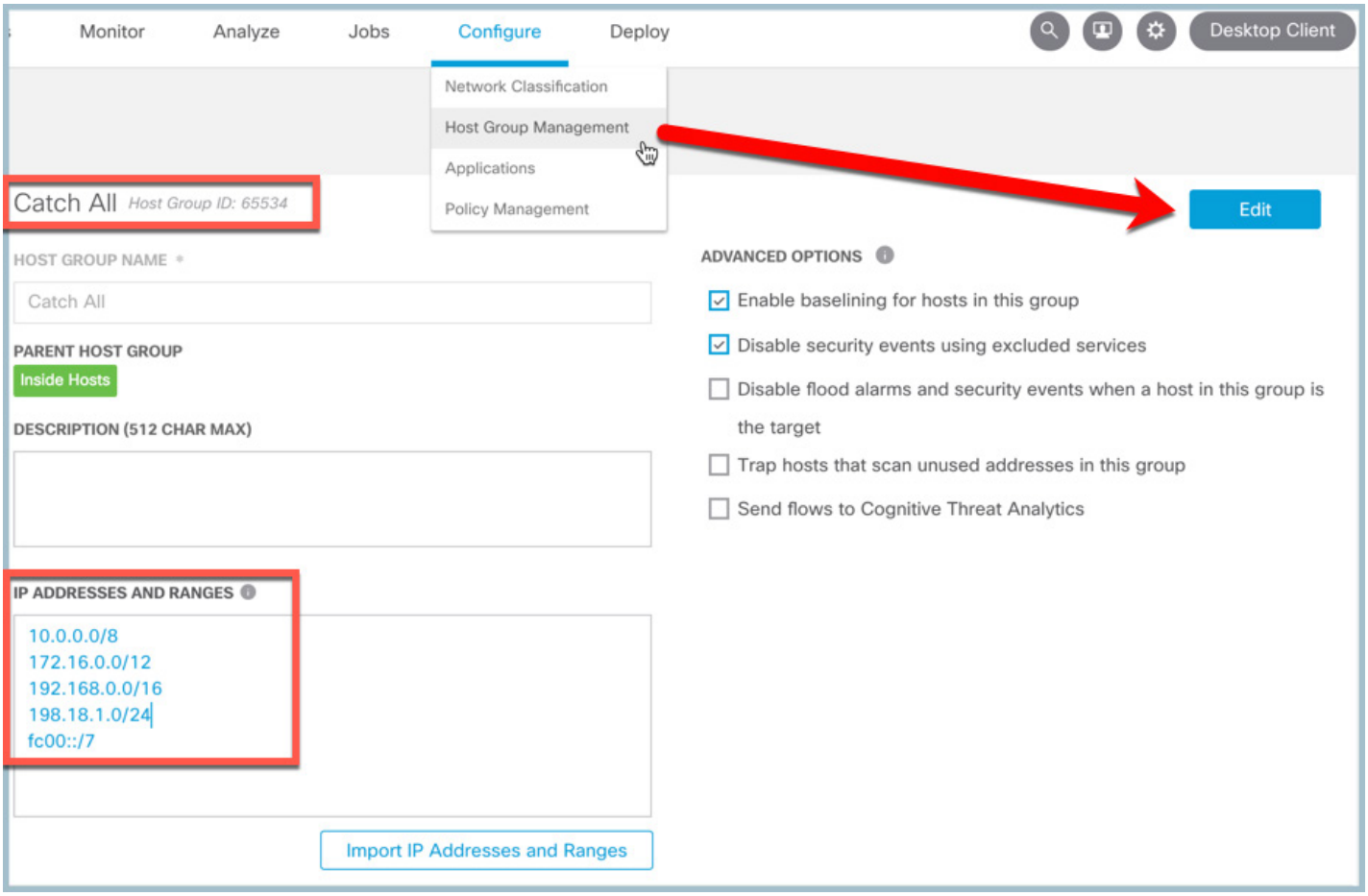
- 疑わしいデータ損失
- 漏洩
- 疑わしい静かな長いフロー
- 疑わしい長いフロー
- ビーコン発信ホスト
- 上位のファイル共有インデックス

フェーズ 1：Stealthwatch に組織が所有する IP スペースを伝える

[内部ホスト（Inside Hosts）] 内の [すべてを捕捉（Catch All）] ホストグループは、組織が所有するすべての IP スペースをすばやく取り込む特殊なグループです。

[すべてを捕捉（Catch All）] には次のものが含まれます。

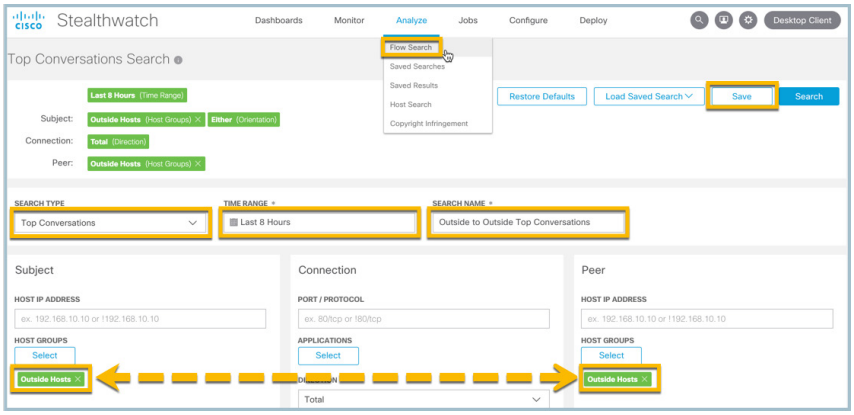
- デフォルトで定義されているすべてのルーティング不可能な IP スペース（RFC1918 および RFC4193）。
- 組織が所有するすべての登録済みパブリック IP スペース（特定の必要あり）。



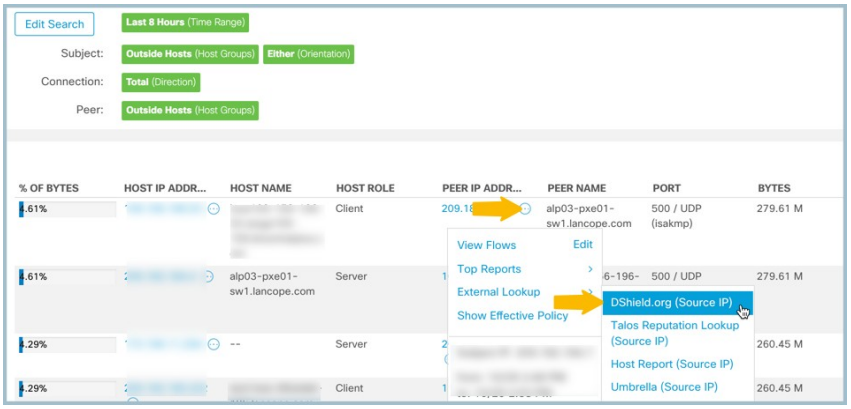
フェーズ 1：Stealthwatch に組織が所有する IP スペースを伝える

組織が所有する IP スペースを分類する簡単な方法の 1 つは、次のとおりです。

- 次の図に示すように、外部から外部への過去 8 時間の [上位カンバセーション（Top Conversations）] を実行します。
- 「Outside to Outside Top Conversations」という名前で検索を保存し、簡単に再実行できるようにします。
- 外部から外部へのトラフィックが表示される場合は、IP 範囲の 1 つを [内部ホスト（Inside Hosts）] に移動する必要があります。



- [上位カンバセーション（Top Conversations）] 内で繰り返し表示される IP アドレスを探し、名前解決を表示して特定します。
- [D-Shield.org ルックアップ（D-Shield.org Lookup）] または [概要（who is）] を実行して組織によって登録されている IP を特定し、完全な CIDR ブロックをキャプチャして [すべてを捕捉（Catch All）] で定義します。



- [すべてを捕捉（Catch All）] ホストグループに、登録されているすべてのパブリック IP スペースを入力します。
- 組織が所有するすべての IP 範囲をキャプチャするまで、上記の操作を繰り返します。

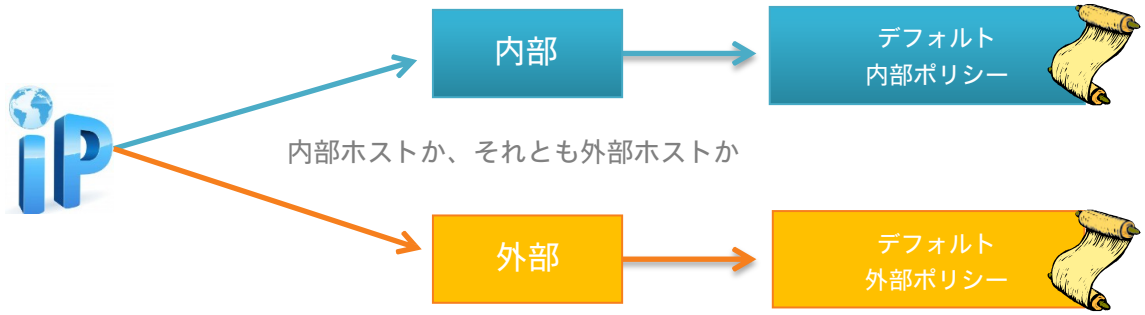
注：外部から外部への IP アドレスを確認する際に、NAT ゲートウェイやプロキシとして使用される IP アドレスが表示されます。適切なポリシーを適用するには、NAT ゲートウェイやプロキシサーバのホストグループに含まれる個々の IP アドレスを分類する必要もあります。

フェーズ 2：ポリシー グループ フレームワークを構築する（機能別グループを使用）

ロールポリシーが機能グループに関連付けられていることを確認する

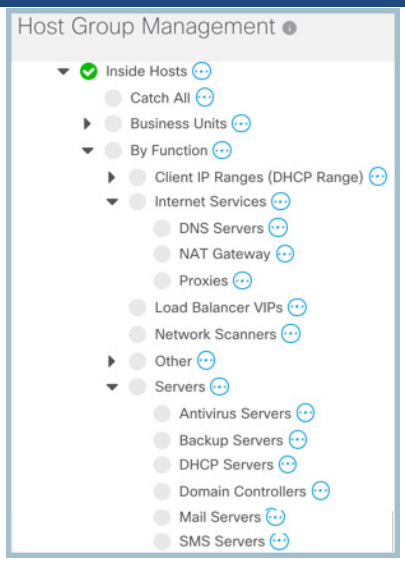
デフォルトから開始します。

- すべてのホストは内部または外部ホストグループ構造の範囲内に属しており、具体的なロールが定義されるまでの間、デフォルトポリシーが割り当てられます。



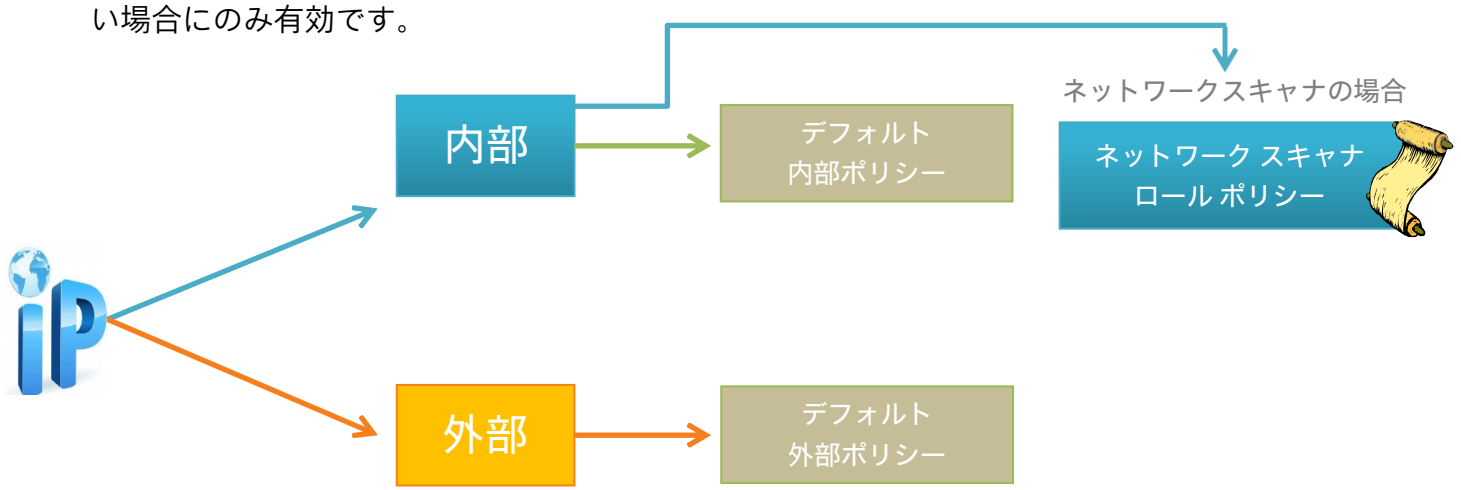
- ポリシーは、ホストグループまたは個々の IP に適用できます。
- **ベストプラクティス**：ロールポリシーがシステムのロール/機能に基づいて関連付けられているホストグループの集合を構築します。

次に、デフォルトの [機能別（By Function）] グループと、機能グループにすでにマッピングされている適切なポリシーを使用したデフォルトロールポリシーのリストを示します。それぞれの機能グループに IP をドロップするだけで、より適切なポリシーを有効にできます。黄色で強調表示されているサーバは、適切なポリシーを適用して、脅威の効果的な検出を促進するために、できるだけ早く分類する必要があります。

デフォルトの機能別グループ	機能別グループにマッピングされるデフォルトのロールポリシー
	• ウイルス対策サーバおよび SMS サーバ • クライアント IP ポリシー • DHCP サーバ • ファイアウォール、プロキシ、および NAT デバイス • ゲストワイヤレス • メールサーバポリシー • ネットワーク管理とスキャナ • セキュリティイベントをテストするためのポリシー • ボットアラームの抑制 • トラップされたホスト - ハニーポットポリシー • 信頼できるインターネットホスト • 信頼できるユーザポリシー • 信頼できないユーザポリシー

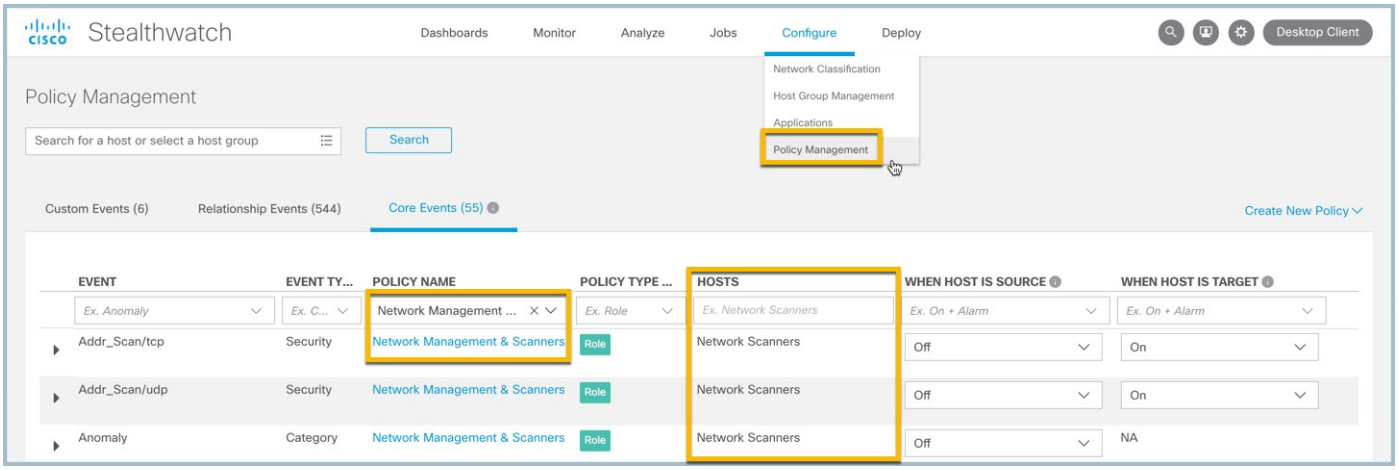
フェーズ 2：ポリシー グループ フレームワークを構築する

- デフォルトの内部ポリシーと外部ポリシーは、ホストにロールポリシーが割り当てられていない場合にのみ有効です。



例：

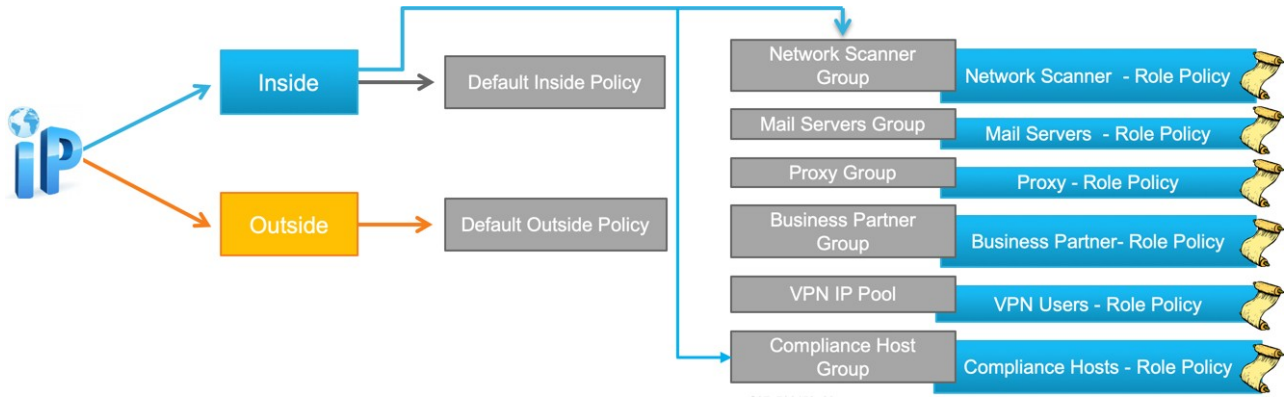
- ネットワークスキャナというホストグループを作成します（バージョン 7.1 にこのグループはデフォルトで存在します）。
- ネットワークスキャナのロールポリシーを作成し、このポリシーにネットワークスキャナグループを割り当てます（このロールポリシーはバージョン 7.1 にすでに存在します）。
- ネットワークスキャナがトリガーするセキュリティイベントを追加し、ポリシーを調整します。以下に示すように、[Addr_Scan/tcp] と [Addr_Scan/udp] を追加して、[ホストが送信元の場合（When Host is Source）] を [オフ（Off）] に設定します。
- ネットワークスキャナで検出されたすべてのフローは引き続き記録されますが、許可されたスキャンに対してアラームは生成されません。



- セキュリティイベントを調整すると、デフォルトで、そのイベントが関与するアラームカテゴリが調整されます。
- 調整を容易にするため、ポリシーをシステムの機能に関連付けるポリシー グループ フレームワークを構築すると便利です。

フェーズ 2：ポリシー グループ フレームワークを構築する

- [機能別（By Function）] のデフォルトがない場合、これは問題になりません。同じシンプルなフレームワークに従ってください。
- 割り当てられたロールポリシーを使用してグループのフレームワークを作成すると、作成中にホストをそれぞれの機能に簡単に移動できます。
- **ヒント**：ホストレポートの [分類（Classify）] ボタンを選択して、事前定義されたホストグループにホストを移動できます。



ベストプラクティス：ポリシーを過剰に考案することがないようにしてください。ホストは、それぞれが独自のロールポリシーを持つ複数のグループのメンバーになることができますが、混乱を避けるため、特定のホストに割り当てられるロールポリシーは 1 つだけにしてください。

Stealthwatch には、カスタム セキュリティ イベントとともに多数のセキュリティイベントが組み込まれているため、あるセキュリティイベントを調整すると、別のイベントによって動作の変更が検出されることになります。

- 同じアラームタイプが 2 つのロールポリシーの一部であるときに、ホストが両方のポリシーの一部である場合、そのアラームはポリシーごとに 1 回ずつ、2 回トリガーされる可能性があります。これを回避するには、機能/ロールグループを統合します。
- アラームがトリガーされて、特定のロールポリシーに追加する必要があるアラームタイプがわかるまで待機します。
- 次のセクションでは、SMC バージョン 7.1 以降にインストールできる可視性評価アプリケーションを使用して、承認済みのスキャナをすばやく分類する方法について説明します。

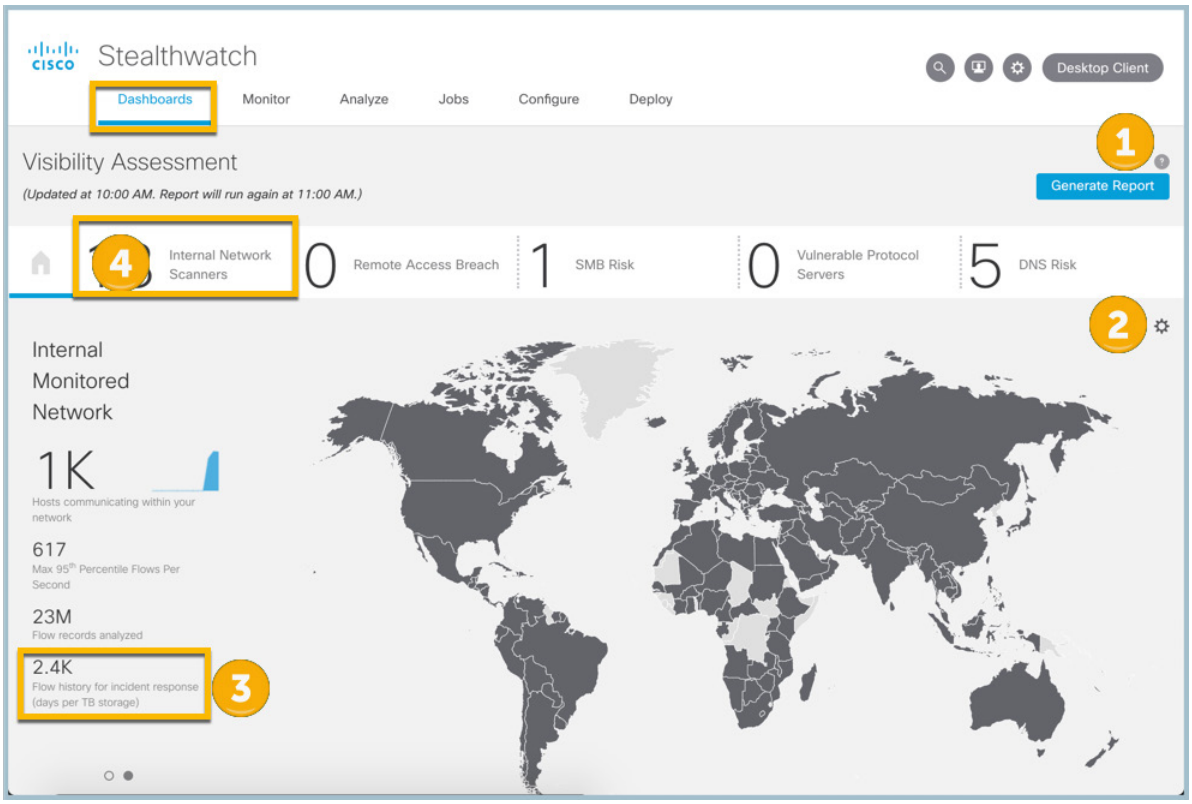
フェーズ 3：既知のスキャナを分類する

可視性アセスメントアプリを使用して、既知のネットワークスキャナをすばやく分類し、マルウェアにすでに感染している可能性のあるシステムを特定します。

- https://stealthwatch.flexnetoperations.com [英語] から可視性アセスメントをダウンロードし、SMC の Central Manager を使用してインストールします。
- アプリがインストールされたら、[ダッシュボード（Dashboards）] メニューから [可視性アセスメント（Visibility Assessment）] を起動し、次の手順を実行して初期設定と分類を行います。

    1. [レポートの生成（Generate Report）] ボタンの上にある [?] をクリックして、オンラインヘルプを選択します。このアプリを使用して内部スキャナやその他のリスクを検出する方法についての詳細を確認できます。
    2. アプリを初めてインストールする場合は、マップの上にある歯車アイコンを選択して、組織が疑わしいと見なす国を指定する必要があります。この操作は、履歴フローを分析して脅威を検出するのに役立ちます。組織がビジネスを行っていない国を選択できます。14 日後に、調査すべき疑わしいトラフィックに関するレポートが送信されます。

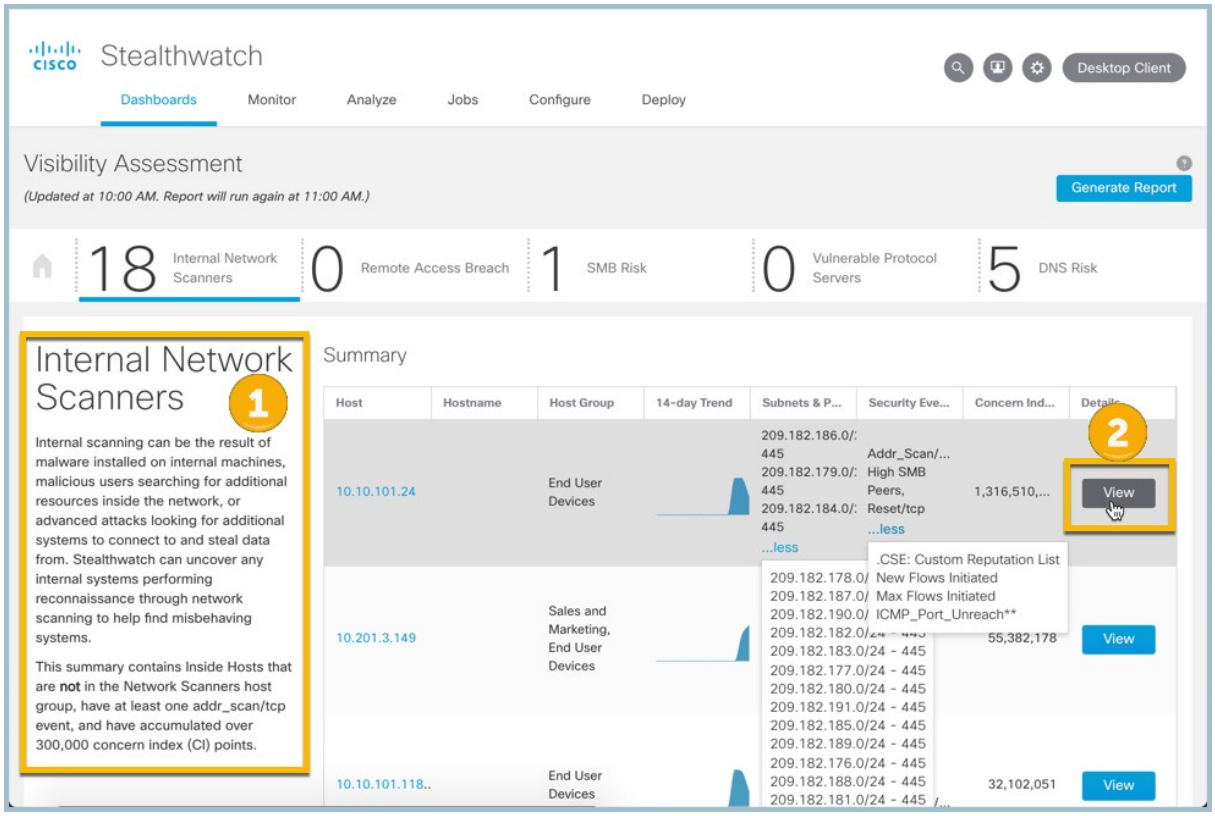
3. 現在のフロー収集レートと割り当てられたディスク容量に基づいて保存されるフロー履歴の量を確認します。
4. [内部ネットワークスキャナ（Internal Network Scanners）] をクリックして、ネットワーク内のホストスキャンのリストを確認します。



フェーズ 3：既知のスキャナを分類する

[内部ネットワークスキャナ（Internal Network Scanners）] レポート内で、次の作業を実行します。

1. このレポートで検出された内容の説明に目を通します。
2. [表示（View）] をクリックして各 IP を調査し、スキャンされているサブネットとポート、トリガーされたセキュリティイベント、および動作が開始されたタイミングを把握します。

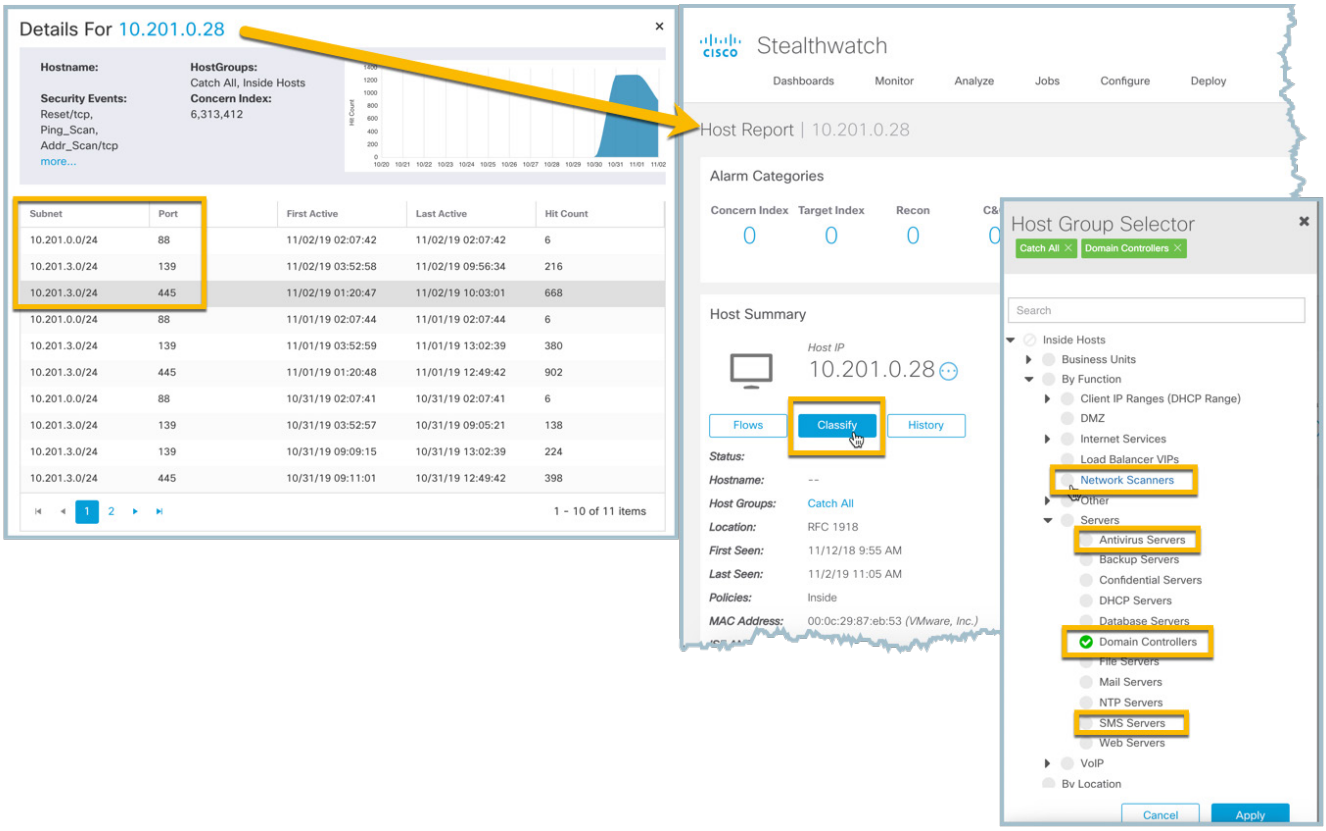


次のホストは、ネットワーク上の多くのホストとの通信に基づくスキャン動作を示します。ホスト名を使用すると、サーバのタイプを判別しやすくなります。以下のすべての共通サーバタイプには、適切なロールポリシーがすでに定義されています。必要な操作は、ホストをそれぞれの [機能別（By Function）] グループに分類することだけです。

- 脆弱性スキャナ
- ウイルス対策サーバ
- SMS サーバ
- DHCP サーバ
- ドメイン コントローラ

フェーズ 3：既知のスキャナを分類する

次の例では、10.201.0.28 が Kerberos（ポート 88）、NetBIOS（ポート 139）、SMB（ポート 445）で承認済みのドメインコントローラとして通信しています。ハイパーリンクの詳細を押して、ホストレポート内の [分類（Classify）] ボタンを選択し、ホストをそれぞれのホストグループに割り当てます。この例では、ホストはドメインコントローラです。分類するプライマリサーバは、承認済みのネットワークスキャナ、管理サーバ、SMS サーバ、およびウイルス対策サーバです。すでにマルウェアに感染しており、調査が必要なホストスキャンが検出される場合があります。



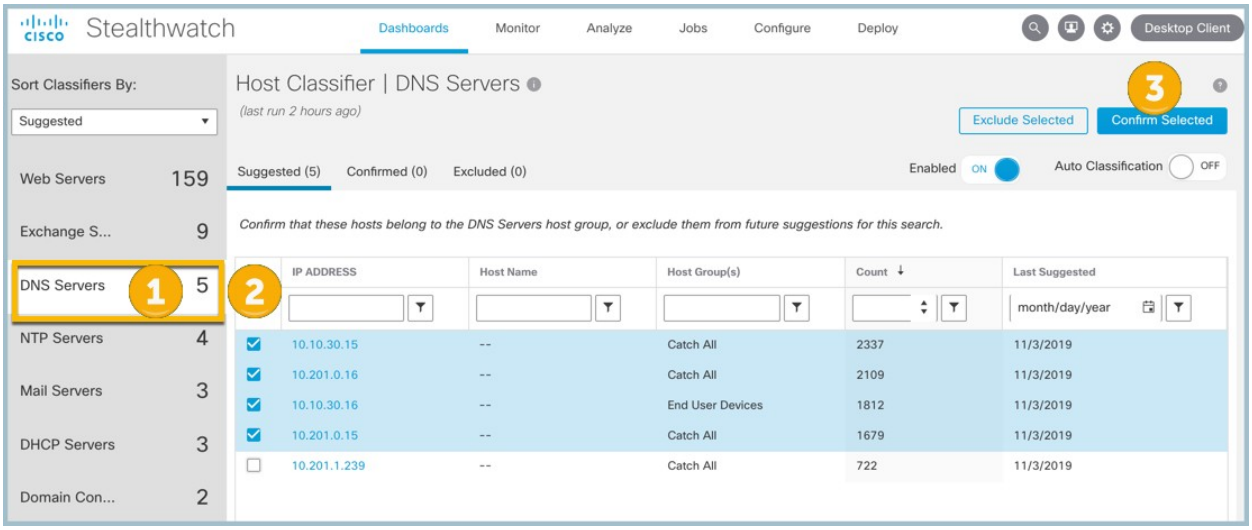
注：可視性アセスメントアプリには、レポートを表示するたびに過去 14 日間の結果が表示されます。分類したホストは、14 日後にエージアウトするまで引き続きレポートに表示されます。初期調整後にアプリをアンインストールして再インストールすると、ホストがすぐに削除され、新しいレポートが開始されます。

フェーズ 4：既知の共通サーバタイプを分類する

ホスト分類アプリを使用して、既知のサーバタイプをすばやく分類します。

- https://stealthwatch.flexnetoperations.com [英語] からホスト分類アプリをダウンロードし、SMC の Central Manager を使用してインストールします。
- アプリがインストールされたら、[ダッシュボード（Dashboards）] メニューから [ホスト分類（Host Classifier）] を起動し、レポート右上の [?] をクリックしてオンラインヘルプを開きます。このアプリを使用してサーバを分類する方法の詳細を確認できます。
- Web サーバと Exchange サーバは情報を提供しますが、主に DNS、NTP、メール、DHCP サーバ、およびドメインコントローラの分類に焦点を当てており、適切な分類が完了する前に多くのアラームを生成する可能性があります。

1. 左側のリストから DNS サーバを選択して開始します。
2. 承認済み DNS サーバである各サーバの横にチェックを付けます。ホスト名を使用すると、サーバのタイプを判別しやすくなります。
3. 承認済みの DNS サーバにチェックを付けたら、[選択対象の確認（Confirm Selected）] を選択します。これにより、適切なロールポリシーが割り当てられた DNS サーバホストグループにこれらのホストが割り当てられます。



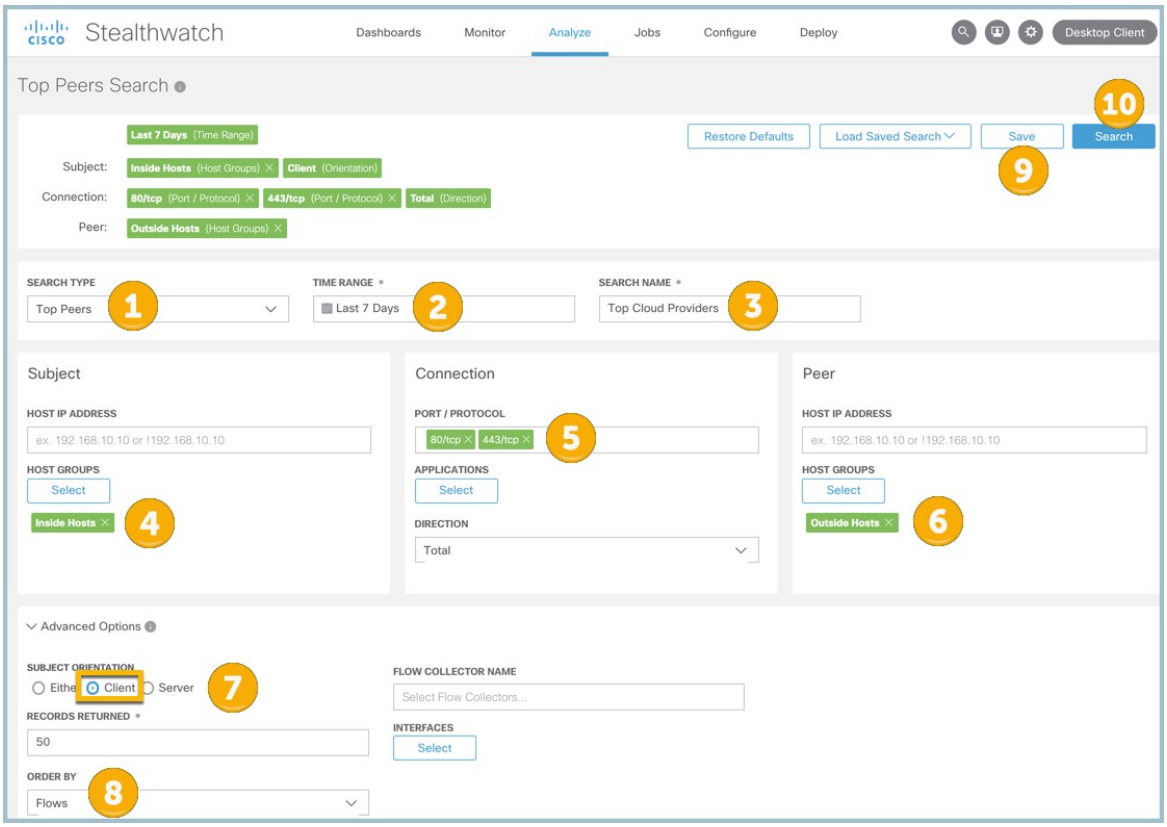
- NTP サーバ、メールサーバ、DHCP サーバ、およびドメインコントローラに対して上記の分類を繰り返します。
- ホスト分類アプリは、エクスポータの新しい集合が展開に追加されるたびに使用できます。

フェーズ 5：クラウドプロバイダーを分類する

[ビジネスパートナー（Business Partners）] または [信頼できるインターネットホスト（Trusted Internet Hosts）] 外部ホストグループ内の一般的なインターネットプロバイダーを分類すると、脅威ではないトラフィックの繰り返しによって発生する不要なアラームを減らすことができます。たとえば、多くの従業員が Facebook で多くの時間を費やしているため、トップクラウドプロバイダーの 1 つとして Facebook を見るのはよくあることです。この演習では、多くの場合、調査が必要な疑わしいトラフィックも検出します。

組織の一般的なクラウドプロバイダーのリストを検索するには、上位ピアレポートを使用します。[分析（Analyze）]、[フロー検索（Flow Search）] に移動し、以下に示すフィルタを定義します。

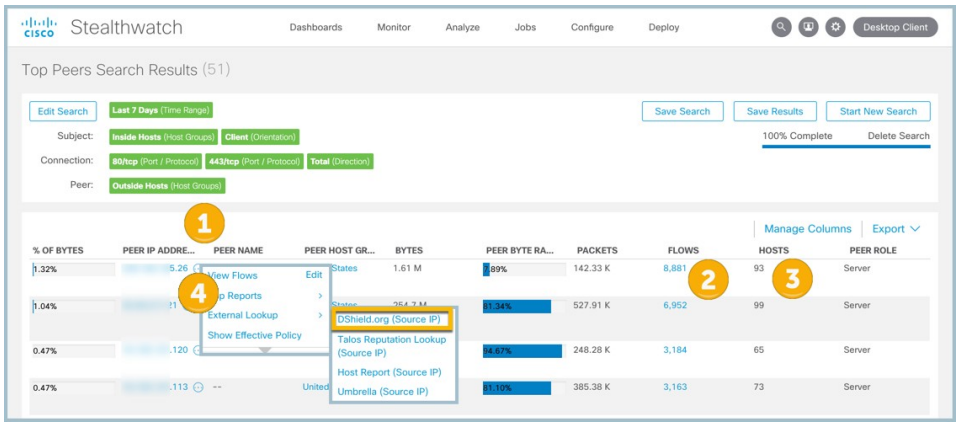
1. [検索タイプ（Search Type）] で [上位ピア（Top Peers）] を選択します。
2. [時間範囲（Time Range）] で [過去 7 日間（Last 7 Days）] を選択します。
3. [検索名（Search Name）] に「Top Cloud Providers」と入力します。
4. [情報カテゴリ（Subject）] として [内部ホスト（Inside Hosts）] を選択します。
5. 最初に Web トラフィックに焦点を当てるには、「80/tip」と入力し、Enter を押します。「443/tcp」と入力し、Enter を押します。
6. [ピア（Peer）] として [外部ホスト（Outside Hosts）] を選択します。
7. [情報カテゴリの方向（Subject Orientation）] で [クライアント（Client）] を選択します。
8. [並べ替え基準（Order By）] で [フロー（Flows）] を選択します。
9. このレポートを後で使用できるようにするには、[保存（Save）] を選択します。
10. [検索（Search）] を選択します。



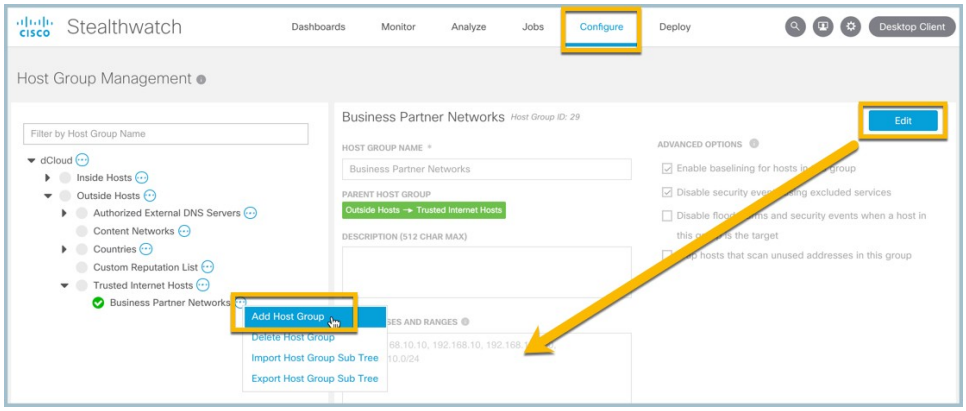
フェーズ 5：クラウドプロバイダーを分類する

次のアラームが内部ホストと外部ホストの間でトリガーされる可能性があります。データ損失の疑い、疑わしい長いフロー、およびビーコン発信ホスト。このレポートの出力を使用して、これらのアラームを表示しない一般的なネットワークの確認と分類を開始します。

1. ピア IP とホスト名を調査して、一般的なトラフィックかどうかを判断します。
2. これらのピアへのフローの数を特定します。
3. これらのピアに接続する内部クライアントの数を特定します。
4. アクションボタンを使用して「DShield.org」ルックアップを実行し、この IP スペースを所有している組織を確認します。



- トラフィックが許可されていると判断した場合は、外部のピアが所有する CIDR ネットワーク範囲全体を「概要（who is）」ルックアップからキャプチャします。
- [ビジネス パートナー ネットワーク（Business Partner Network）] で、[設定（Configure）]、[ホストグループ管理（Host Group Management）] を開き、[ホストグループの追加（Add Host Group）] を実行します。[信頼できるインターネットホスト（Trusted Internet Hosts）] で直接実行することもできます。[編集（Edit）] を選択し、共通ピアネットワークのネットワーク範囲全体に貼り付けて、変更を保存します。この操作により、誤検出を減らすための適切なポリシーが継承されます。トラフィックが数週間収集された後と、エクスポータの新しいグループが展開に追加されるたびに、この演習を繰り返します。



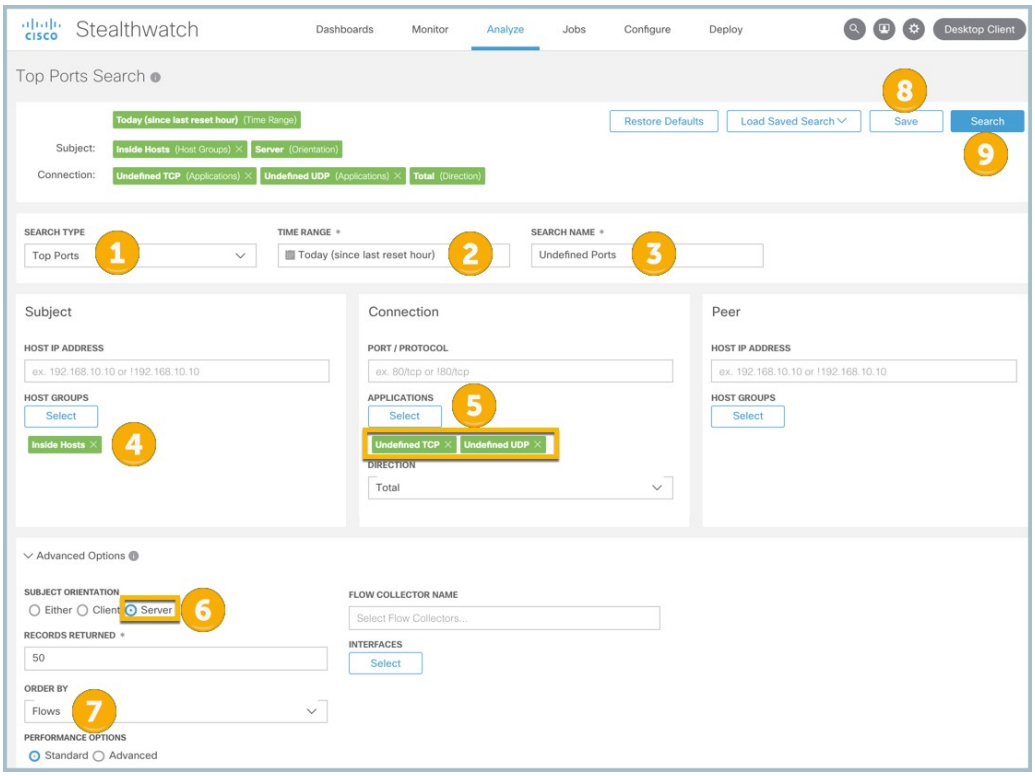
フェーズ 6：未定義アプリケーションを分類する

Stealthwatch 内では、すでに何百ものデフォルトアプリケーションが定義されています。とはいえ、どの組織にも、ネットワーク内で実行されるカスタムサービスとアプリケーションがあります。組織の既知のアプリケーションを分類することで、システムがクライアント/サービスの決定をよりインテリジェントに行えるようになり、アラームの改善が促進されます。

分析とフロー検索レポートを以下のフィルタとともに使用して、未定義の上位ポートを特定します。

1. [検索タイプ（Search Type）] で [上位ポート（Top Ports）] を選択します。
2. [時間範囲（Time Range）] で [今日（Today）] を選択します。
3. [検索名（Search Name）] に「Undefined Ports」と入力します。
4. [情報カテゴリ（Subject）] として [内部ホスト（Inside Hosts）] を選択します。
5. アプリケーションリストから [未定義 TCP（Undefined TCP）] と [未定義 UDP（Undefined UDP）] を選択します。
6. [情報カテゴリの方向（Subject Orientation）] で [サーバ（Server）] を選択します。
7. [並べ替え基準（Order By）] で [フロー（Flows）] を選択します。

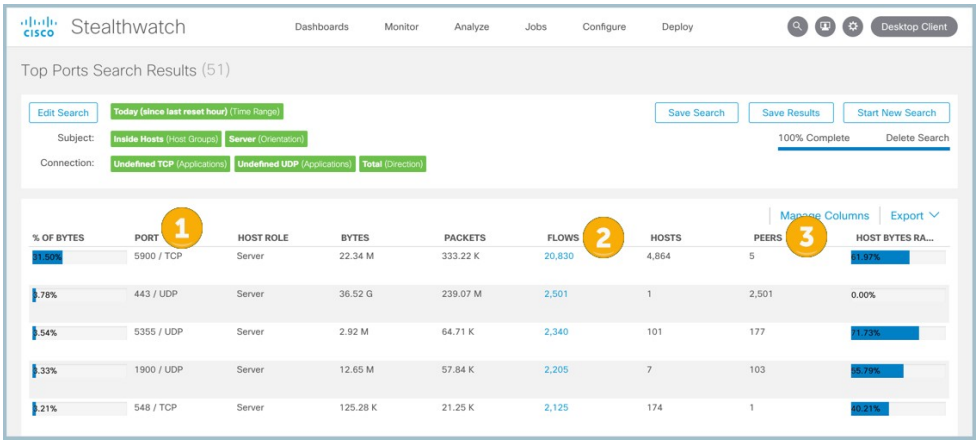
8. このレポートを後で使用できるようにするには、[保存（Save）] を選択します。
9. [検索（Search）] を選択します。



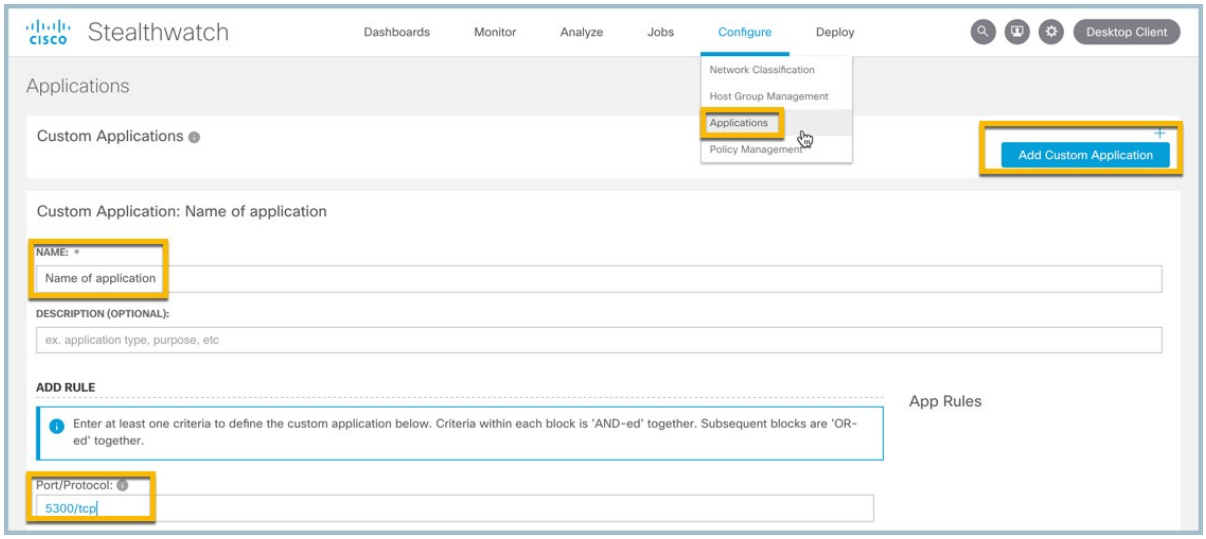
フェーズ 6：未定義アプリケーションを分類する

学習する未定義のアプリケーションのリストを確認します。

1. 使用されているポート。
2. 観測されたフローの数。
3. このポートを使用しているクライアントの数。



- ラベルを付ける必要があるポートごとに、[設定（Configure）] > [アプリケーション（Applications）] の順に移動します。
- [カスタムアプリケーションの追加（Add Custom Application）] を選択します。
- アプリケーションの名前と説明を入力します。
- アプリケーションに関連付けられているポートを定義します。
- 変更を保存します。



- 上記のプロセスを繰り返して、未定義のアプリケーションを分類します。
- 未定義のポートごとにこのプロセスを実行する必要はありません。分類する必要があるのは、ネットワーク内で使用される共通ポートのみです。