脅威の検出

脅威検出のポートスキャンディテクタは、あらゆるタイプのトラフィックでポートスキャンアクティビティを検出および防止し、最終的な攻撃からネットワークを保護するために設計されたメカニズムです。ポートスキャントラフィックは、許可されたトラフィックと拒否されたトラフィックの両方で効率的に検出できます。

ポートスキャンとは、攻撃者が攻撃の準備段階として使用することが多いネットワーク偵察の形式です。ポートスキャンでは、攻撃者はホストがサポートするネットワークプロトコルまたはサービスのタイプを特定し、細工されたパケットを標的のホストに送信します。攻撃者は多くの場合、ホストが応答するパケットを調べることで、ホストでどのポートが開かれているか、そして開かれているポートでどのアプリケーションプロトコルが実行されているかを、直接あるいは推論によって判断できます。

ポートスキャンの検出と防止

脅威検出を使用して、ポートスキャンアクティビティを特定します。システムを使用してポートスキャンを検出し、検出時にイベントを発行できます。必要に応じて、スキャナを自動的にブロックしてポートスキャンを防止するようにシステムを設定することもできます。ポートスキャンを防止する場合、システムはイベントを送信し、設定された期間攻撃者をブロックします。

ポートスキャン検出の事前定義された感度レベル

検出設定を構成するときは、以下の事前定義された感度レベルから選択します。[カスタム（Custom）] を除き、各レベルには、設定された時間間隔内にスキャンする必要があるポート

（TCP/UDP）、プロトコル（IP）、またはホスト（TCP/UDP/IP/ICMP）の数に対する各プロトコルの値が事前に設定されています（秒単位）。また、すべてのタイプのスキャン/スイープが有効になります。

（注） ポート/プロトコルをカウントするときに、現在のパケットのポート/プロトコルが前のパケットと異なる場合、脅威検出によって番号が増加します。たとえば、10 個のポート セットでランダムに接続を開くアプリケーションがある場合、スキャンされるポートの合計数が増えすぎて、インターバル内にポート番号を超えてしまう可能性があります。システムは一意のポートだけをカウントするわけではありません。

間隔内でこの数を超えると、スキャン攻撃を示している可能性があります。ポートスキャンイベントは、移動時間間隔枠で、ポート/プロトコル/ホストの数が超過した場合にのみ生成されます。

- [低（Low）]：このレベルでは、ポートスキャン検出に最短の時間枠を使用し、ポート/プロトコル/ホスト数を高くします。したがって、最もアグレッシブなスキャナのポートスキャンイベントのみが表示されます。誤検出を抑えるためには、この感度レベルを選択します。ただし、特定のタイプのポートスキャン（時間をかけたスキャン、フィルタ処理されたスキャン）が見逃される可能性があることに注意してください。
  - **間隔**（TCP/UDP/IP/ICMP）：60 秒。
  - **TCP/UDP ポートスキャンのポート数**：120。
  - **TCP/UDP ポートスイープのホスト数**：180。
  - **IP プロトコルスキャンのプロトコル数**：30。
  - **IP プロトコルスイープのホスト数**：25。
  - **ICMP ホスト スイープのホスト数**：50。
- [中（Medium）]：このレベルでは、間隔とポート/プロトコル/ホスト数の両方に中程度の値が使用されます。ただし、ネットワークアドレス変換プログラムやプロキシなど、ホストが非常にアクティブな場合は、誤検出が発生する可能性があります。このようなホストはスキャナ無視リストに追加します。これはデフォルトの感度レベルであり、初期使用に適しています。
  - **間隔**（TCP/UDP/IP/ICMP）：90 秒。
  - **TCP/UDP ポートスキャンのポート数**：90。
  - **TCP/UDP ポートスイープのホスト数**：150。
  - **IP プロトコルスキャンのプロトコル数**：15。
  - **IP プロトコルスイープのホスト数**：20。
  - **ICMP ホストスイープのホスト数**：30。

- [高（High）]：このレベルでは、ポートスキャン検出にはるかに長い時間枠を使用し、ポート/プロトコル/ホストの数を低くします。このレベルでは、最もアグレッシブでないポートスキャン/スイープのイベントも表示される可能性が高いため、すべての攻撃者を認識できる確率が高まります。一方、このレベルでは発行されるポートスキャンイベントの数が最も多くなり、誤検出の数が最大になる可能性があります。
  - **間隔**（TCP/UDP/IP/ICMP）：600 秒（10 分）。
  - **TCP/UDP ポートスキャンのポート数**：60。
  - **TCP/UDP ポートスイープのホスト数**：100。
  - **IP プロトコルスキャンのプロトコル数**：10。
  - **IP プロトコルスイープのホスト数**：10。
  - **ICMP ホストスイープのホスト数**：20。
- [カスタム（Custom）]：事前定義された感度レベルとは異なる設定を行う場合、または特定のタイプのスキャン/スイープを無効にする場合、レベルは自動的にカスタムに切り替わります。オプションを調整する場合は、まず目的に最も近いレベルを選択し、必要に応じて値を編集します。

ポートスキャン防止のベストプラクティス

ポートスキャン防止モードでは、意図しないトラフィックの停止が発生する場合があります。防止モードでは、ホストは設定された期間中、すべてのプロトコルでネットワークをさらに詳しくスキャンすることができません。正当なトラフィックがブロックされないように、検出と防止のパラメータを注意して確認してください。

防止モードでポートスキャンを設定する前に、以下の手順を実行することを強く推奨します。

1. 検出モードでポートスキャンの使用を開始します。
2. 生成されたポートスキャンイベントを確認します。
3. 感度レベル、モニタリング対象ネットワーク、スキャナの無視リスト、およびターゲットの無視リストを調整します。事前定義された感度レベルが状況に適していない場合は、必要に応じてカスタム設定を構成します。
4. 誤検出がなくなり、イベントレートがネットワーク内のポートスキャンの正確な状況を反映するまで、このプロセスを繰り返します。識別された残りのスキャナをブロックしても問題がないことを確認します。

脅威検出の要件と前提条件

モデルのサポート

バージョン 7.2 以降および Snort 3 を実行している Threat Defense 。

サポートされるドメイン

任意

ユーザの役割

管理者

アクセス管理者

ネットワーク管理者

脅威検出のガイドラインと制限事項

- 脅威検出には Snort 3 が必要です。管理対象デバイスは、バージョン 7.2 以降である必要があります。Snort 2、または 7.2 より前のバージョンのデバイスでは、NAP ポリシーを使用してポートスキャンを設定できます。脅威検出機能は、NAP ポリシーのポートスキャン機能と同じではないことに注意してください。アクセス コントロール ポリシーに割り当てられている Snort 3 を使用していない、または バージョン 7.2 より前のデバイスがある場合、それらのサポートされていないデバイスに脅威検出設定は展開されません。
- 7.1 以前を実行しているデバイスの NAP ポリシーでポートスキャンを設定した場合、その設定は、7.2 へのアップグレード時に脅威検出機能に変換されません。脅威検出を手動で設定する必要があります。NAP と脅威検出のポートスキャンオプションは似ていますが、全く同じではありません。
- 脅威検出を設定すると、NAP ポリシーのポートスキャン設定はすべて無視され、脅威検出をサポートするデバイスでは設定されません。
- Snort 3 の NAP ポートスキャン機能は、バージョン 7.2 以降のデバイスでは常に無視されます。ポートスキャンを設定するには、Threat Defense 設定を使用する必要があります。
- 脅威検出は、デバイスを通過するトラフィックに対してのみ機能します。デバイス宛てのトラフィックに対しては機能しません。
- 高可用性設定では、ポートスキャン統計はスタンバイ装置に同期されません。ただし、ブロックされたホストは同期され、フェールオーバー時に期間が終了するまでブロックされ続けます。
- （Threat Defense バージョン 7.2 ～ 7.7 を実行しているデバイス）。クラスタ内のノードの場合、個々のクラスタ ノードで検出と防御が行われます。つまり、ノード B がホストか

らのトラフィックを検出してブロックした場合、ポートスキャン統計はクラスタノード間で同期されないため、ノード A はそのアクションを認識しません。

- インラインセットの場合、または等コストマルチパス（ECMP）トラフィックゾーンの一部として設定されているインターフェイスの場合、検出と防御はゾーンレベルで行われます。ホストのポートスキャン統計は、ゾーンのすべてのインターフェイスにわたって蓄積されます。同様に、ホストが設定されたしきい値を超えると、対応するゾーンのすべてのインターフェイスでブロックされます。
- 脅威検出機能によって生成されるポートスキャン イベントは、Snort がポートスキャンで発行するものと同じですが、イベントを取得するためにポートスキャンの侵入ルールを有効にする必要はありません。脅威検出は、侵入ポリシーの実装に関係なく機能します。

ポートスキャンの検出と防止の設定

ポートスキャンとは、攻撃者が攻撃の準備段階として使用することが多いネットワーク偵察の形式です。ポートスキャンでは、攻撃者はホストがサポートするネットワークプロトコルまたはサービスのタイプを特定し、細工されたパケットを標的のホストに送信します。攻撃者は多くの場合、ホストが応答するパケットを調べることで、ホストでどのポートが開かれているか、そして開かれているポートでどのアプリケーションプロトコルが実行されているかを、直接あるいは推論によって判断できます。

脅威検出を有効にして、ポート スキャン アクティビティを監視できます。また、必要に応じて一定期間スキャナを自動的にブロックすることができます。

始める前に

FQDN、ワイルドカードマスク、any、any-ipv4、および any-ipv6 ネットワークオブジェクトは、ポートスキャン設定ではサポートされていません。これらのオブジェクトは、[監視（Monitor）]、[スキャナを無視（Ignore Scanner）]、[ターゲットを無視（Ignore Target）]、および [除外（Exclude）] フィールドには表示されません。

手順

ステップ 1 アクセス コントロール ポリシーのエディタで、パケットフロー行の最後にある [詳細（More）] ドロップダウン矢印から [詳細設定（Advanced Settings）] をクリックします。次に、[Threat Detection] の横にある [編集（Edit）]（ ） をクリックします。

ステップ 2 [脅威の検出（Threat Detection）] ウィンドウで、 [ポートスキャンモード（Portscan mode）] を選択します。

- [無効（Disable）]：脅威検出をオフにします。これは、デフォルトのモードです。[デフォルトに戻す（Revert to Defaults）] をクリックして、この未設定の状態に戻すことができます。

- [検出（Detection）]：ポートスキャン検出を実行しますが、問題に対するアラートのみを送信します。潜在的な攻撃者に対してアクションは実行しません。過剰な誤検出を避けるために、Threat Detection の設定を微調整するまで、最初はこのモードを使用することをお勧めします。
- [防止（Prevention）]：ポートスキャン検出を実行し、特定されたスキャナ、つまりポートスキャンを実行しているホストをアクティブにブロックします。

ステップ 3 [トラフィック選択（Traffic Selection）] オプションを設定します。

トラフィック選択オプションは、モニタリング対象のネットワーク、モニタリング対象の接続タイプ、およびスキャナまたはターゲットホストをモニタリング対象のネットワークから除外するかどうかを決定します。デフォルトでは、システムはすべてのネットワークで許可された接続をモニタリングします。

- [トラフィックの検出（Detection On Traffic）]：ポートスキャン アクティビティをモニタリングする接続タイプ（[許可された（Permitted）]、[拒否された（Denied）]、または [すべて（All）] のトラフィックを選択します。デフォルトは [許可された（Permitted）] です。
- [モニタリング（Monitor）]：ポートスキャンまたはスイープアクティビティをモニタリングするネットワークを定義するネットワークオブジェクトを選択します。デフォルトは、すべてのネットワーク（IPv4 または IPv6）です。このオプションを使用して、スキャンを信頼できないネットワークに制限できます。
- [スキャナを無視（Ignore Scanner）]：モニタリング対象のネットワークの範囲内から、無視する必要があるホストまたはネットワークを定義するネットワークオブジェクトを選択します。たとえば、ネットワークをテストするために独自のスキャナを設定した場合は、スキャナのアドレスを除外して、アドレスに関する不要なレポートを回避できます。モニタリング対象ネットワークの外部にあるアドレスはすでに無視されているため、含めないでください。
- [ターゲットを無視（Ignore Target）]：ターゲット（ポートスキャンまたはスイープの対象）として無視する必要があるホストまたはネットワークを定義するネットワークオブジェクトを選択します。

ステップ 4 [設定（Configuration）] タブをクリックし、スキャン感度レベルを選択します。

事前定義された感度レベル（[低（Low）]、[中（Medium）]、および [高（High）]）を設定することで、ポートスキャンオプションの値を徐々にアグレッシブにできます。たとえば、[低（Low）] を選択すると表示されるポートスキャンイベントが少なくなり、[中（Medium）] または [高（High）] を選択した場合よりも攻撃者を見逃す可能性が高くなります。一方、[高（High）] を選択するとより多くのイベントが表示され、誤検出が増える可能性があります。デフォルトのレベルは [中（Medium）] です。レベルについての詳細は、ポートスキャン検出の事前定義された感度レベル （1 ページ） を参照してください。

レベルを選択すると、プロトコルセクション内に関連する値（**TCP**、**UDP**、**IP**、および**ICMP**）が表示されます。プリセット値のいずれかを変更するか、スキャンのタイプを無効にすると、感度モードは自動的に [カスタム（Custom）] に変更されます。

各プロトコルセクション内のオプションは次のとおりです。

- [間隔（Interval）]：ポートスキャンまたはポートスイープの設定値を超過する時間範囲（秒単位）。たとえば、90 秒を選択し、TCP ポートスキャンポートの数として 60 を選択した場合、スキャナがポートスキャンと見なされるには、90 秒以内にホスト上の 60 ポートを試行する必要があります。システムは、指定された間隔内にポート、プロトコル、またはホスト（ポートスイープの場合）の数を超えた場合にのみ、イベントを生成します。

  30～600秒の範囲を指定できます。期間が長いほど、ホストがスキャナとして識別される可能性が高くなります。

- [ポートスキャン（TCP/UDP）（Portscan (TCP/UDP)）]：単一のホストに対してポートスキャンをモニタリングするかどうかを選択し、ポートスキャン攻撃として見なされるために間隔内にスキャンする必要があるポートの数を指定します。指定できる範囲は 1 ー 256 です。

- [ポートスイープ（TCP/UDP）（Portsweep (TCP/UDP)）]：複数のホストに対してポートスイープをモニタリングするかどうかを選択し、ポートスイープ攻撃として見なされるために間隔内に特定のポートでスキャンする必要があるホストの数を指定します。指定できる範囲は 1 ー 256 です。

- [プロトコルスキャン（IP）（Protocol Scan (IP)）]：単一のホストに対してプロトコルスキャンをモニタリングするかどうかを選択し、プロトコルスキャン攻撃として見なされるために間隔内にスキャンする必要があるプロトコルの数を指定します。指定できる範囲は 1 ー 255 です。

- [プロトコルスイープ（IP）（Protocol Sweep (IP)）]：複数のホストに対してプロトコルスイープをモニタリングするかどうかを選択し、プロトコルスイープ攻撃として見なされるために間隔内に特定のプロトコルでスキャンする必要があるホストの数を指定します。指定できる範囲は 1 ー 256 です。

- [ホストスイープ（ICMP）（Hostsweep (ICMP)）]：複数のホストに対して ICMP ホストスイープをモニタリングするかどうかを選択し、ホストスイープ攻撃として見なされるために間隔内にスキャンする必要があるホストの数を指定します。指定できる範囲は 1 ー 256 です。

ステップ 5 防止モードを選択した場合は、[防止（Prevention）]タブをクリックし、オプションを設定します。

防止モードでは、ホストは設定された期間中、すべてのプロトコルでネットワークをさらに詳しくスキャンすることを自動的にブロックされます。正当なトラフィックがブロックされないように、検出と防止のパラメータを注意して確認してください。

- [除外（Exclude）]：モニタリング対象ネットワークの範囲内から、自動ブロッキングから除外するホストまたはネットワークを定義するネットワークオブジェクトを選択します。これらのホストがスキャン検出パラメータを超過しても、システムはそれらをブロックしません。

- [期間（Duration）]：自動的にブロックされたスキャナホストがあらゆる種類のトラフィックをデバイスを介して送信できないようにする期間（秒単位）。期間が終了すると、ホス

トは自動的にクリアされ、再びデバイスを介してトラフィックを送信できるようになります。指定できる範囲は 600 ー 2592000 秒です。デフォルトは 3600 秒（1 時間）です。

ホストのブロックを手動で解除する必要がある場合は、ホストをブロックしているファイアウォールに SSH で接続し、**clear threat-detection portscan attacker** コマンドを使用します。

ステップ 6 [OK] をクリックして、脅威検出の設定を保存します。

ステップ 7 [保存（Save）] をクリックして、アクセス コントロール ポリシーを保存します。

次のタスク

設定変更を展開します設定変更の展開を参照してください。

脅威検出のモニタリング

ここでは、ポートスキャン アクティビティをモニタリングする方法について説明します。

ポートスキャンアラートの表示

ポートスキャンアクティビティは、既存のポートスキャン固有の侵入イベントを通じて警告されます。ジェネレータ ID（GID）122 および SID 1 ～ 27 の Snort ID を持つ侵入イベントが生成されます。これらのイベントの場合、（port_scan）文字列がイベントメッセージの先頭に追加されます。イベントには、アラートをトリガーした統計情報を含むパケットデータとともにパケット情報が含まれます。

ポートスキャンイベントを表示するには、**[分析（Analysis）] > [侵入（Intrusion）] > [イベント（Events）]** に移動します。

ポートスキャンは、侵入ポリシーまたは NAP 設定に関係なく、これらのイベントを発行します。イベントは、関連するプロトコルに設定された時間間隔内に、スキャナがさまざまなタイプのスキャンまたはスイープに設定されたポート/プロトコル/ホストの数を超えた場合にのみ発行されます。1 つのホストからのポートスキャンは、しきい値に達するとすぐに、設定された間隔ごとに 1 つのイベントを生成します。同じホストが同じ間隔で新しいポートスキャンを開始した場合、イベントは報告されません。

次の表に、発生する可能性のあるイベントを示します。

表 *1:* ポートスキャンイベント

ポートスキャン タイプ	侵入イベント
TCP 通常、デコイ、分散スキャン	122:1（port_scan）TCP ポートスキャン
TCP ポートスイープ	122:3（port_scan）TCP ポートスイープ

ポートスキャン タイプ	侵入イベント
TCP 分散型スキャン	122:4（port_scan）TCP 分散型ポートスキャン
IP 通常、デコイ、分散プロトコルスキャン n	122:9（port_scan）IP プロトコル スキャン
IP プロトコルスイープ	122:11（port_scan）IP プロトコルスイープ
IP 分散型スキャン	122:12（port_scan）IP 分散型プロトコル スキャン
UDP 通常、デコイ、分散スキャン	122:17（port_scan）UDP ポートスキャン
UDP ポートスイープ	122:19（port_scan）UDP ポートスイープ
UDP 分散型スキャン	122:20（port_scan）UDP 分散型ポートスキャン
ICMP スイープ	122:25（port_scan）ICMP スイープ
ポートスキャン ブロック	122:100（port_scan）ポートスキャン アクティビティによりホストがブロックされました

ファイアウォールでのポートスキャンのモニタリング

ポートスキャンをモニタリングするには、デバイスCLIにログインして以下のコマンドを使用します。

- **show threat-detection portscan** ［**attacker** ｜ **target** ｜ **shun**］

  スキャナのIPアドレス、回避（ブロック）されたスキャナ、およびスキャンまたはスイープの対象となったホストを表示します。

- **show threat-detection portscan statistics** ［**host** ［*ipv4_address* ｜ *ipv6_address*］］［**protocol** {**tcp** ｜ **udp** ｜ **ip** ｜ **icmp**} ］

  ポートスキャンシステムに関連する統計情報を表示します。ホスト、プロトコル、またはホストとプロトコルを指定して、出力をフィルタ処理して目的の情報を得ることができます。

- **clear threat-detection portscan** ［**attacker** ｜ **target** ｜ **shun**］［*ipv4_address mask* ｜ *ipv6_address/prefix* ］

  スキャナ（攻撃者）または特定されたターゲットのブロックを手動で解除します。すべての攻撃者、ターゲット、または回避されたホストをクリアするには、パラメータを指定せずにコマンドを入力します。

- **clear threat-detection portscan statistics** ［**host** ［*ipv4_address* ｜ *ipv6_address*］］［**protocol** {**tcp** ｜ **udp** ｜ **ip** ｜ **icmp**} ］

  ポートスキャンに関連する統計情報を消去して、このデバイスを介したスキャンの現在の状態をより明確に確認できるようにします。すべての統計情報をクリアするには、パラ

メータを指定せずにコマンドを入力します。または、ホスト、プロトコル、またはホストとプロトコルを指定して、指定された項目のみをリセットします。

ホストのブロック解除

脅威検出を防御モードに設定し、攻撃者ではないことが判明しているホストをシステムがブロックする場合は、期間が終了してホストのブロックが自動的に解除される前に、ホストのブロックを手動で解除できます。

ホストのブロックを手動で解除するには、ホストがブロックされているデバイスのCLIにログインし、**clear threat-detection portscan attack** コマンドを入力します。次に例を示します。

```
> clear threat-detection portscan attacker 10.2.0.100 255.255.255.255
1 tracker object deleted and 1 shun entry removed
```

防止設定の除外リストにホスト IP を追加することを検討してください。

脅威検出の履歴

特長	最小 Firewall Management Center	最小 Firewall Threat Defense	説明
ポートスキャン検出の改善。	7.2	Snort 3 を実行する 7.2	改良されたポートスキャンディテクタを使用すると、ポートスキャンを検出または防止するようにシステムを簡単に設定できます。保護するネットワークを絞り込んだり、感度を設定したりできます。Snort 2 を実行しているデバイス、およびバージョン 7.1 以前を実行しているデバイスの場合、ポートスキャン検出には引き続きネットワーク分析ポリシーを使用します。 新規/変更された画面：[脅威検出（Threat Detection）] をアクセス コントロール ポリシーの [詳細（Advanced）] タブに追加しました。 新規/変更されたコマンド：**clear threat-detection portscan**, **show threat-detection portscan**。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。