Netskope.NSK200.v2025-04-19.q55

試験コード:	NSK200
試験名称:	Netskope Certified Cloud Security Integrator (NCCSI)
認定資格:	Netskope
無料問題数:	55
バージョン:	v2025-04-19
アクセス数:	722
ページビュー数:	550
https://www.jpnpdf.com/Netskope.NSK200.v2025-04-19.q55-mondaishu.html	

最新問題: **1**
ある市では、許可申請書など、さまざまなフォームを使用しています。これらのフォームには、市民の個人情報や財務情報が含まれています。リモートの従業員はこれらのフォームをダウンロードし、市民と直接協力してフォームに記入します。市は、特定のフォームを識別して監視し、従業員が記入済みのフォームをダウンロードできないようにしたいと考えています。
このタスクを実行するにはどの機能を使用しますか?
A. 完全データー致 (EDM)
B. 正規表現 (regex)
C. 文書フィンガープリンティング
D. 光学文字認識 (OCR)
Answer: C (メーッセージを残す**)**
説明
市が使用する特定のフォームを識別して監視し、職員が記入済みのフォームをダウンロードできないようにするには、ドキュメントフィンガープリンティングを使用する必要があります。ドキュメント フィンガープリンティングは、ドキュメントの内容と構造に基づいてドキュメントに固有の署名を作成できる機能です。この署名を使用して、元のドキュメントと類似または同一の他のドキュメントを照合できます3。サンプル ドキュメントをアップロードするか、クラウド サービスから 1 つ選択することで、Netskope でドキュメント フィンガープリンティング プロファイルを作成できます4。その後、データ保護ポリシーでこのプロファイルを使用して、フィンガープリントに一致するドキュメントにブロック、アラート、検疫などのアクションを適用できます5。したがって、オプション C は正しく、他のオプションは間違っています。参考資料: ドキュメント フィンガープリンティング - Netskope Knowledge Portal、ドキュメント フィンガープリンティング プロファイルの作成 - Netskope Knowledge Portal、データ保護のポリシーの追加 - Netskope Knowledge Portal

最新問題: **2**
Netskope サポートは、パフォーマンスを向上させるために DTLS を有効にすることを推奨しました。UDP ポート 443 トラフィックを許可するファイアウォール ルールを追加しました。これらの設定は、Netskope テナントで有効にするとどの構成要素の一部になりますか?
A. SSL復号化ポリシー

B. クライアント構成
C. リアルタイム保護ポリシー
D. ステアリング構成
Answer: B (メーッセージを残す**)**
説明
DTLS (Datagram Transport Layer Security) は、UDP 経由で安全な通信を提供するプロトコルです。これは、Netskope テナントのクライアント構成設定で有効にできるオプションです。DTLS を有効にすると、特に高遅延またはパケット損失のシナリオで Netskope クライアントのパフォーマンスが向上します。DTLS は、Netskope テナントのさまざまな構成要素であるリアルタイム保護ポリシー、SSL 復号化ポリシー、またはステアリング構成とは関係ありません。参照: クライアント構成設定 3、Netskope クライアント パフォーマンス 4

最新問題**: 3**
会社のリスク チームは、営業チームからカスタム Web アプリケーションへのトラフィックは Netskope で検査すべきではないと判断しました。Web アプリケーションへのその他のすべてのトラフィックは引き続き検査する必要があります。
このシナリオでは、このタスクをどのように達成しますか?
A. ポリシー ページでユーザー グループとドメインを使用して、復号化しないポリシーを作成します。
B. ポリシーページでアプリケーションを使用して復号化しないポリシーを作成し、グループのステアリング例外を作成します。
C. ポリシー ページで宛先 IP とアプリケーションを使用して、復号化しないポリシーを作成します。
D. ポリシー ページで、ソース IP とアプリケーションを使用して、復号化しないポリシーを作成します。
Answer: (解答を表示する**)**
営業チームからカスタム Web アプリケーションへのトラフィックが Netskope によって検査されないようにするには、ポリシー ページでユーザー グループとドメインを使用して、復号化しないポリシーを作成する必要があります。復号化しないポリシーを使用すると、リアルタイム保護ポリシー3 を介して Netskope によってさらに分析されないように暗号化したままにしておきたいトラフィックを指定できます。ユーザー グループの条件を使用して営業チームのメンバーを照合し、ドメインの条件を使用してカスタム Web アプリケーションを照合できます。このようにすると、営業チームからカスタム Web アプリケーションへのトラフィックのみが復号化から除外され、Web アプリケーションへの他のすべてのトラフィックは引き続き検査されます。

最新問題**: 4**
Netskope DLP ソリューションを使用しています。承認されていないクラウド ストレージ ソリューションにアップロードしたファイル内の有効なクレジットカード番号がポリシー違反をトリガーしていないことに気付きました。このトラフィックの Skope IT アプリケーション イベントは表示されますが、DLP アラートは表示されません。
このシナリオではどの記述が正しいでしょうか?
A. Netskope クライアントが有効になっていません。
B. 重大度しきい値をより高い値に設定しました。
C. Netskope クライアントは有効になっていますが、SaaS アプリケーションの API 保護は構成されていません。
D. クレジットカード番号は、16 桁の連続番号ではなく、スペースまたはダッシュ区切りで入力されます。
Answer: (解答を表示する**)**
説明

このシナリオで正しい記述は D です。クレジットカード番号は、16 桁の連続した数字ではなく、スペースまたはダッシュの区切り文字を使用して入力されています。これが、ファイル内の有効なクレジットカード番号が Netskope DLP によるポリシー違反をトリガーしない理由の 1 つです。Netskope DLP は、データ識別子を使用して、ファイルおよびネットワーク トラフィック内の機密データを検出します。データ識別子は、正規表現、チェックサム、キーワードなどに基づいてデータ パターンを照合する定義済みまたはカスタムのルールです1。クレジットカード番号のデータ識別子は、Luhn アルゴリズム チェックに合格する 16 桁の連続した数字と一致します2。クレジットカード番号が 1234-5678-9012-3456 や 1234 5678 9012 3456 のようにスペースまたはダッシュの区切り文字を使用して入力されている場合、データ識別子と一致しないため、ポリシー違反はトリガーされません。この問題を解決するには、クレジットカード番号から区切り文字を削除するか、区切り文字付きのクレジットカード番号と一致するカスタム データ識別子を作成します3。したがって、オプション D は正解で、他のオプションは不正解です。参考資料: データ識別子 - Netskope Knowledge Portal、クレジットカード番号 - Netskope Knowledge Portal、カスタム データ識別子の作成 - Netskope Knowledge Portal

最新問題**: 5**
会社では、異常なユーザーアクティビティがあったかどうかを知りたいと考えています。UI で、Skope IT -> アラートに移動します。この情報を見つけるために、どの 2 種類のアラートをフィルタリングしますか? (2 つ選択してください。)
A. アラートタイプ = uba
B. アラートタイプ = 異常
C. アラートの種類 = マルウェア
D. アラートタイプ = ポリシー
Answer: A,B (メーッセージを残す**)**
異常なユーザー アクティビティを識別するには、「uba」(ユーザー ビヘイビア分析) と 「異常」でアラートをフィルターします。UBA と異常アラートは、異常なアクティビティや潜在的に危険なアクティビティの指標となる、通常のユーザー ビヘイビアからの逸脱を強調表示します。

最新問題**: 6**
Netskope のファイルハッシュ リストの目的は何ですか?
A. カスタム マルウェア検出プロファイルで参照されるブロックリストと許可リストのエントリを構成します。
B. URL を許可またはブロックするために使用されます。
C. Netskope が検査できるファイルの種類を提供します。
D. クライアント脅威エクスプロイト防止 (CTEP) を提供します。
Answer: (解答を表示する**)**
説明
Netskope のファイル ハッシュ リストの目的は、カスタム マルウェア検出プロファイルで参照されるブロック リストと許可リストのエントリを構成することです。ファイル ハッシュ リストは、組織内で許可またはブロックするファイルを表す MD5 または SHA-256 ハッシュのコレクションです。ファイル プロファイルを追加するときにファイル ハッシュ リストを作成し、組織内のファイルの許可リストまたはブロック リストとして使用できます1。その後、マルウェア検出プロファイルを作成するときにファイル ハッシュ リストを選択できます2。

最新問題**: 7**

セキュリティ インシデント対応チームから、マルウェアの疑いのあるファイルの MD5 ハッシュが提供されます。このファイルに誰が遭遇したか、脅威はどこから始まったかについての洞察を提供するよう求められます。これらの質問の答えを見つけるために、どの 2 つの Skope IT イベント テーブルを検索しますか? (2 つ選択してください)。
A. アプリケーションイベント
B. ネットワークイベント
C. アラート
D. ページイベント
Answer: A,C (メーッセージを残す**)**
説明
セキュリティ インシデント対応チームから提示された質問の回答を見つけるには、Skope IT のアプリケーション イベント テーブルとアラート テーブルを検索する必要があります。アプリケーション イベント テーブルには、アップロード、ダウンロード、共有など、ユーザーが実行したクラウド アプリケーション アクティビティの詳細が表示されます。ファイルの MD5 ハッシュでアプリケーション イベント テーブルをフィルター処理すると、誰がこのファイルに遭遇したか、どのクラウド サービスからダウンロードされたかを確認できます1。アラート テーブルには、DLP、脅威保護、異常検出など、ユーザーによってトリガーされたポリシー違反の詳細が表示されます。ファイルの MD5 ハッシュでアラート テーブルをフィルター処理すると、このファイルが Netskope によってマルウェアとして検出されたかどうか、どのようなアクションが実行されたかを確認できます2。したがって、オプション A と C は正しく、他のオプションは正しくありません。参考資料: アプリケーション イベント - Netskope ナレッジ ポータル、アラート - Netskope ナレッジ ポータル

最新問題**: 8**
特定の Skope IT アプリケーション イベント クエリを作成し、テナントにログインするたびにクエリを自動的に実行して結果を表示するようにします。
このシナリオで正しい記述はどれですか? (2 つ選択してください。)
A. ライブラリからウォッチリスト ウィジェットをホームページに追加します。
B. カスタム Skope IT ウォッチリストをレポートにエクスポートし、毎日実行するようにスケジュールします。
C. カスタム Skope IT ウォッチリストを保存し、フィルターを管理して他のユーザーと共有します。
D. Skope IT クエリをカスタム ウォッチリストに追加します。
Answer: C,D (メーッセージを残す**)**
Skope IT クエリをカスタム ウォッチリストに追加すると、クエリを保存して簡単にアクセスできるようになります。ウォッチリストを保存してフィルターを管理すると、必要に応じてさらにカスタマイズしたり、組織内の他のユーザーと共有したりすることもできます。

最新問題**: 9**
マルウェア検出プロファイルを作成するときに選択されるオブジェクトはどれですか?
A. DLP プロファイル
B. ファイルプロファイル
C. ドメインプロファイル
D. ユーザープロフィール
Answer: B (メーッセージを残す**)**

ファイル プロファイルは、マルウェア検出プロファイルの作成に使用できるファイル ハッシュのリストを含むオブジェクトです。ファイル プロファイルは、ファイルが無害か悪意があるかに応じて、許可リストまたはブロックリストとして構成できます。ファイル プロファイルは、[設定] > [ファイル プロファイル] ページ 1 で作成できます。マルウェア検出プロファイルは、Netskope がマルウェア インシデントを処理する方法を定義する一連のルールです。マルウェア検出プロファイルは、[ポリシー] > [脅威からの保護] > [マルウェア検出プロファイル] ページ 2 で作成できます。マルウェア検出プロファイルを作成するには、Netskope マルウェア スキャン オプションとともに、ファイル プロファイルを許可リストまたはブロックリストとして選択する必要があります。その他のオプションは、マルウェア検出プロファイルの作成時に選択できるオブジェクトではありません。

最新問題**: 10**
SCIM プロビジョニングを使用して Okta から Netskope ユーザーをプロビジョニングしていますが、ユーザーがテナントに表示されません。このシナリオでは、正確性を確認するために、まず Okta でどの 2 つの Netskope コンポーネントを検証する必要がありますか?
（2つ選択してください。）
A. IdP エンティティ ID
B. OAuthトークン
C. Netskope SAML証明書
D. SCIM サーバー URL
Answer: B,D (メーッセージを残す**)**
SCIM プロビジョニングを使用して Okta から Netskope ユーザーをプロビジョニングし、ユーザーがテナントに表示されない場合は、正確性を確認するために最初に Okta で検証する必要がある 2 つの Netskope コンポーネントは、B. OAuth トークンと D. です。SCIM サーバー URL。OAuth トークンは、Okta が Netskope SCIM サーバーで認証し、ユーザー プロビジョニング操作を実行できるようにする認証情報です4。SCIM サーバー URL は、Okta が Netskope SCIM サーバーと通信してユーザー データを送信するために使用するエンドポイントです5。SCIM プロビジョニングが機能するには、これらのコンポーネントの両方が Okta で正しく構成されている必要があります。これらは、Netskope UI の [設定] > [ツール] > [ディレクトリ ツール] > [SCIM 統合] にあります6。したがって、オプション B と D は正しく、その他のオプションは間違っています。参考資料: SCIM ベースのユーザー プロビジョニング - Netskope Knowledge Portal、Netskope + Okta ユース ケース: SCIM を使用したユーザーのプロビジョニングとグループの管理 - Netskope、Netskope パートナー Okta - Netskope

最新問題**: 11**
自己署名 SSL 証明書を使用して、パブリック ホスティング サービスに開発 Web サーバーを展開しました。
いくつかのトラブルシューティングを行った結果、Netskope クライアントが有効になっていると、SSL 経由で Web サーバーにアクセスできないことが判明しました。デフォルトの Netskope テナント ステアリング構成が設定されています。
このシナリオでは、どの 2 つの設定がこの動作を引き起こしていますか? (2 つ選択してください。)
A. SSL ピン留め証明書がブロックされています。
B. 信頼されていないルート証明書はブロックされます。
C. 不完全な証明書信頼チェーンがブロックされています。
D. 自己署名サーバー証明書がブロックされています。
Answer: B,D (メーッセージを残す**)**
説明

デフォルトの Netskope テナント ステアリング構成では、信頼されていないルート証明書と自己署名サーバー証明書がブロックされます。これらの設定は、中間者攻撃を防ぎ、SSL 接続の有効性を確保することを目的としています。ただし、自己署名 SSL 証明書を使用する開発 Web サーバーへのアクセスも防止します。Web サーバーへのアクセスを許可するには、設定を変更するか、Web サーバー ドメインに例外を追加する必要があります。

最新問題: **12**
IT ディレクターは、Netskope クライアントに障害が発生したときに組織の Web トラフィックがブロックされるかどうかの確認を求めています。この状況では、フェール クローズ ステータスを確認するにはどうすればよいでしょうか。
A. マウスを使用して Netskope クライアント アイコンを右クリックします。
B. nsdebuglog.log を確認します。
C. アプリケーション イベントを表示します。
D. ユーザー設定を確認します。
Answer: B (メーッセージを残す**)**
フェール クローズ ステータスを確認する方法は B です。nsdebuglog.log を確認します。nsdebuglog.log は、Netskope クライアントのステータス、構成、イベント、エラーなどの情報を含むログ ファイルです。nsdebuglog.log ファイルを確認し、「failCloseStatus」という行を探すことで、フェール クローズ ステータスを確認できます。
「1」。これは、Netskope クライアントのフェール クローズ オプションが有効になっていることを示します4。フェール クローズ オプションは、Netskope クライアントに障害が発生したり、Netskope クラウドへの接続が失われたりした場合に、すべての Web トラフィックをブロックできる機能です5。したがって、オプション B が正しく、他のオプションは正しくありません。参照: Netskope クライアントのトラブルシューティング - Netskope Knowledge Portal、クライアント構成 - Netskope Knowledge Portal

最新問題: **13**
組織には 3 つの主要な拠点があり、各拠点には 30,000 台のホストがあります。セキュリティのために、iPsec トンネルを使用して Netskope を展開する予定です。
このシナリオで接続を成功させるために考慮すべき 2 つのことは何ですか? (2 つ選択してください。)
A. 使用中のブラウザ
B. オペレーティング システム
C. 冗長POP
D. ホストの数
Answer: C,D (メーッセージを残す**)**
このシナリオでセキュリティのために IPSec トンネルを使用して Netskope を展開する場合、接続を成功させるために考慮すべき 2 つの点は、C. 冗長 POP と D. ホストの数です。冗長 POP は、Netskope クラウド プラットフォームをホストする地理的に分散されたデータ センターである Point of Presence です。POP の 1 つで障害または停止が発生した場合に IPSec トンネルの高可用性と回復力を確保するには、冗長 POP を検討する必要があります。ネットワークから異なる POP への複数の IPSec トンネルを構成し、BGP などの動的ルーティング プロトコルを使用してトラフィックの負荷分散とフェイルオーバーを行うことができます1。ホストの数とは、クラウド サービスにアクセスするために IPSec トンネルを使用するデバイスまたはエンドポイントの数です。IPSec トンネルの帯域幅とスループットの要件を見積もり、トラフィック量を処理できる適切な POP を選択するには、ホストの数を考慮する必要があります。Netskope 帯域幅計算ツールを使用して、ホストの数、場所、クラウド サービスに基づいて帯域幅とスループットを見積もることができます2。

したがって、オプション C と D は正解であり、他のオプションは不正解です。参考資料: IPSec - Netskope Knowledge Portal、Netskope Bandwidth Calculator

最新問題**: 14**
顧客は、すべてのアプリケーションを Microsoft 365 と Azure に移行しています。適切なプラクティスとポリシー (またはインライン トラフィック) が導入されていますが、再構成を継続的に検出し、コンプライアンス標準を適用したいと考えています。
どの 2 つのソリューションが要件を満たすでしょうか? (2 つ選択してください。)
A. Netskope SaaS セキュリティ態勢管理
B. Netskope クラウド信頼度指数
C. Netskope リスクインサイト
D. Netskope 継続的セキュリティ評価
Answer: A,D (メーッセージを残す**)**
説明
Microsoft 365 および Azure アプリケーションのコンプライアンス標準を継続的に検出して適用するには、お客様は Netskope SaaS Security Posture Management (SSPM) と Netskope Continuous Security Assessment (CSA) を使用する必要があります。Netskope SSPM を使用すると、お客様は Microsoft 365 などの SaaS 環境におけるセキュリティ、アクセス許可、アクセス関連の問題を監視、評価し、対処することができます。Netskope SSPM は、SaaS アプリの設定をセキュリティ ポリシーや業界ベンチマーク (CIS、PCI-DSS、NIST、HIPAA、CSA、GDPR、AIPCA、ISO など) と比較することで、セキュリティ ポスチャを継続的にチェックします。また、管理対象アプリに接続されているサードパーティ アプリの可視性と制御も提供します1。Netskope CSA を使用すると、お客様は Azure などの IaaS 環境における構成ミスを検出し、監査し、修正することができます。Netskope CSA は、業界標準、CIS ベンチマーク、規制フレームワークに照らしてクラウド構成を継続的に監視および監査します。また、パブリック クラウドを脅威やデータ損失から保護するためのリアルタイムのインライン保護も提供します2。したがって、オプション A と D は正解であり、他のオプションは不正解です。参考資料: SaaS セキュリティ ポスチャ管理 - Netskope、パブリック クラウド セキュリティ ソリューション - Netskope

最新問題**: 15**
学習者は、Netskope DLP ポリシーのうち、最も多くのインシデントを生み出しているポリシーを調査するように求められます。このシナリオでは、次の 2 つの記述のうち正しいものはどれですか? (2 つ選択してください。)
A. Skope IT アプリケーション タブには、上位 5 つの DLP ポリシーが一覧表示されます。
B. 分析機能を使用して、トリガーされた上位の平均DLPポリシーを確認できます。
C. レポートまたは高度な分析を使用してレポートを作成できます。
D. Skope IT Alerts タブには、上位 5 つの DLP ポリシーが一覧表示されます。
Answer: B,C (メーッセージを残す**)**
Netskope DLP ポリシーのどれが最も多くのインシデントを生み出しているかを調査するには、次の 2 つのステートメントが当てはまります。
* 分析機能を使用して、トリガーされた上位 5 つの DLP ポリシーを確認できます。分析機能を使用すると、カスタム ダッシュボードとウィジェットを作成して、データを視覚化して調査できます。DLP ポリシー ウィジェットを使用すると、特定の期間に最も多くのインシデントを生成した上位 5 つの DLP ポリシーを確認できます3。
* レポートまたは高度な分析を使用してレポートを作成できます。レポート機能を使用すると、定義済みのテンプレートまたはカスタム クエリに基づいて、スケジュールされたレポートまたはアドホック レポートを作成できます。ポリシー別の DLP インシデント テ

ンプレートを使用して、DLP ポリシーごとのインシデント数を示すレポートを生成できます4。高度な分析機能を使用すると、データに対して SQL クエリを実行し、結果を CSV または JSON ファイルとしてエクスポートできます。DLP_INCIDENTS テーブルを使用して、ポリシー名とインシデント数でデータをクエリできます5。
他の 2 つの記述は、次の理由により正しくありません。
* Skope IT アプリケーション タブには、上位 5 つの DLP ポリシーは表示されません。Skope IT アプリケーション タブには、組織のクラウド アプリの使用状況とリスクの概要が表示されます。DLP ポリシーやインシデントに関する情報は表示されません6。
* Skope IT Alerts タブには、上位 5 つの DLP ポリシーは表示されません。Skope IT Alerts タブには、DLP、脅威保護、IPS などのさまざまなポリシーとプロファイルによって生成されたアラートが表示されます。ポリシーごとのインシデント数は表示されず、インシデントごとのアラート数のみが表示されます7。

最新問題**: 16**
組織内でネイティブ Dropbox クライアントが継続的に使用されていることがわかりました。Dropbox は企業承認アプリケーションではありませんが、Dropbox の使用を禁止したくはありません。ただし、その使用状況を把握できるようにする必要があります。
A. Windows および Mac のステアリング例外アクションを変更して、トンネル モードを使用し、SSO サービスの送信元 IP アドレスとして Netskope を設定します。
B. 既存のテナント ステアリング例外構成を変更して、Dropbox ネイティブ アプリケーションをブロックし、ユーザーに Dropbox ウェブサイトの使用を強制します。
C. テナント ステアリング SSL 構成からすべての Dropbox エントリを完全に削除します。
D. Dropbox アプリケーションを含む宛先場所の新しいテナント ステアリング例外タイプを作成します。
Answer: D (メーッセージを残す**)**
可視性を維持しながらDropboxの使用を許可するには、新しいテナントステアリング例外タイプを作成します。
Dropbox の 送信先の場所」。これにより、要求に応じてブロックを回避しながら Dropbox のトラフィックの可視性が有効になります。

最新問題**: 17**
一部のユーザーから OneDrive および SharePoint Online へのアクセスに関する問題が報告されている Microsoft の問題をトラブルシューティングしています。構成では、Netskope クライアントがほとんどのユーザーに対して展開されアクティブになっていますが、一部の Linux マシンは GRE トンネルを使用して Netskope にルーティングされています。問題のトラブルシューティングを開始するには、すべてのユーザーに対して検査を無効にする必要があります。
このシナリオでは、このタスクをどのように達成しますか?
A. Microsoft 365 を分離するためのリアルタイム保護ポリシーを作成します。
B. Microsoft 365 App Suite の Do Not Decrypt SSL」ポリシーを作成します。
C. Microsoft 365 ドメインのステアリング例外を作成します。

D. OneDrive の 暗号化解除しない」SSL ポリシーを作成します。
Answer: B (メーッセージを残す)
説明
Microsoft 365 にアクセスするすべてのユーザーに対する検査を無効にするには、Microsoft 365 App Suite の Do Not Decrypt SSL」ポリシーを作成する必要があります。このポリシーにより、アクセス方法 (Netskope クライアントまたは GRE トンネル) に関係なく、Netskope が Microsoft 365 アプリのトラフィックを復号化して分析することが防止されます3。このポリシーでは、SNI ベースのポリシーの適用も許可されますが、リアルタイム保護ポリシーによる詳細な分析は実行されません4。
したがって、オプション B が正しく、他のオプションは誤りです。参考資料: SSL 復号化のポリシーを追加する - Netskope Knowledge Portal、デフォルトの Microsoft appsuite SSL は復号化しないルール - Netskope Community

最新問題**: 18**
ドメイン コントローラーからユーザーとグループの情報を定期的に取得し、その情報を Netskope クラウドのテナント インスタンスに投稿する際に問題が発生しています。トラブルシューティング プロセスを開始するには、この状況で最初に何を調査しますか?
A. オンプレミス ログ パーサー
B. ディレクトリインポーター
C. DNS コネクタ
D. ADコネクタ
Answer: B (メーッセージを残す)
説明
ディレクトリ インポーターは、ドメイン コントローラーに接続し、ユーザーとグループの情報を定期的に取得して、Netskope クラウド 1 のテナント インスタンスにその情報を投稿する Netskope アダプターのコンポーネントです。このプロセスで問題が発生した場合、最初に調査する必要があるのはディレクトリ インポーター自体です。ディレクトリ インポーター サービスのステータス、構成ファイル、ログ、およびドメイン コントローラーと Netskope クラウド 2 への接続を確認できます。したがって、オプション B が正しく、他のオプションは正しくありません。参照: ディレクトリ インポーターの構成 - Netskope ナレッジ ポータル、ディレクトリ インポーターのトラブルシューティング - Netskope ナレッジ ポータル

最新問題**: 19**
展示品をレビューします。

個人医療情報 (PHI) のデータ損失防止 (DLP) を使用して SMTP 電子メールをスキャンするための新しいリアルタイム保護ポリシーを作成するように求められます。範囲は、Microsoft Exchange Online から外部の受信者に送信される電子メールのみに制限されます。

A. Web アクセス ポリシー

B. メール送信ポリシー

C. CTEPポリシー

D. DLP ポリシー

Answer: B (メーッセージを残す**)**

電子メール送信」ポリシーは、Exchange Online からの SMTP トラフィックなどの送信メールにデータ損失防止制御を適用するように特別に設計されています。このポリシー タイプにより、送信メールのコンテンツをきめ細かく制御でき、PHI データの DLP ポリシーへの準拠が保証されます。

最新問題: **20**
マルウェア検出プロファイルを作成するときに選択されるオブジェクトはどれですか?
A. DLP プロファイル
B. ファイルプロファイル
C. ドメインプロファイル
D. ユーザープロフィール
Answer: B (メーッセージを残す**)**
説明
ファイル プロファイルは、マルウェア検出プロファイルの作成に使用できるファイル ハッシュのリストを含むオブジェクトです。ファイル プロファイルは、ファイルが無害か悪意があるかに応じて、許可リストまたはブロックリストとして構成できます。ファイル プロファイルは、[設定] > [ファイル プロファイル] ページ 1 で作成できます。マルウェア検出プロファイルは、Netskope がマルウェア インシデントを処理する方法を定義する一連のルールです。マルウェア検出プロファイルは、[ポリシー] > [脅威からの保護] > [マルウェア検出プロファイル] ページ 2 で作成できます。マルウェア検出プロファイルを作成するには、Netskope マルウェア スキャン オプションとともに、ファイル プロファイルを許可リストまたはブロックリストとして選択する必要があります。その他のオプションは、マルウェア検出プロファイルの作成時に選択できるオブジェクトではありません。

最新問題: **21**
会社から、Netskope を使用して Crowdstrike などのエンドポイント検出および対応 (EDR) ベンダーと統合するように求められています。
脅威データの統合と共有を成功させるために必要な 2 つの要件はどれですか? (2 つ選択してください。)
A. 修復プロファイル
B. デバイスの分類
C. API クライアント ID
D. カスタム ログ パーサー
Answer: (解答を表示する**)**
Crowdstrike などの EDR ベンダーと統合するには、認証とデータ共有のための API クライアント ID が必要です。
脅威が検出されたときに実行できる自動アクションを定義し、エンドポイントの脅威に効果的に対応するためにも、修復プロファイルが必要です。

最新問題: **22**
ある会社では、ユーザーが管理対象のラップトップで OneDrive にアクセスできるようにしています。個人の OneDrive にドキュメントをアップロードすることは、会社のポリシーに反します。会社は、顧客の機密データを保護するためにこのポリシーを実施する必要があります。
このポリシーを実施する 2 つの方法は何ですか? (2 つ選択してください。)
A. 識別されたすべてのドキュメントのアップロードをブロックする DLP ポリシーを作成します。
B. 企業の OneDrive インスタンスにのみドキュメントのアップロードを許可する DLP ポリシーを作成します。

C. 企業の OneDrive の新しいアプリケーション インスタンスを作成します。
D. すべての文書に指紋を採取して、会社が保護する必要のあるすべての文書のカタログを作成します。
Answer: A,B (メーッセージを残す**)**
機密文書のアップロードをブロックするか、企業の OneDrive のみに制限する DLP ポリシーを設定することで、企業はポリシーを適用できます。これらのポリシーにより、機密データは承認された環境内に留まり、個人のインスタンスにアップロードされないことが保証されます。

最新問題: **23**
展示品をレビューします。

Exhibit

```
11-2-2021 19:01:14.1858782 P-76 T-5 DEBUG Total number of groups to search for 1
11-2-2021 19:01:14.1858782 P-76 T-5 DEBUG The users search filter is (&
(objectClass=user)
(memberOf:1.2.840.113556.1.4.1941:=CN=Internet,CN=Users,DC=axefield,DC=local))
11-2-2021 19:01:14.2015365 P-76 T-5 INFO No of users in group
CN=Internet,CN=Users,DC=axefield,DC=local are 3
11-2-2021 19:01:14.2172676 P-76 T-5 DEBUG email for user: tony@axefield.local
11-2-2021 19:01:14.2172676 P-76 T-5 WARNING No mail ID for the user
CN=clarke,CN=Users,DC=axefield,DC=local, skipping user
```

ユーザー Clarke の Netskope クライアントがインストール後に無効な状態のままになっている問題をトラブルシューティングしています。さまざまなログを確認した後、問題の原因になりそうな点に気付きました。この図は、nsADImporterLog.log からの抜粋です。
展示物に関して、何が問題なのでしょうか?
A. クライアントは管理者権限でインストールされませんでした。
B. Active Directory ユーザーは Netskope テナントに同期されていません。
C. これは正常です。有効になるまでに最大 1 時間かかる場合があります。
D. クライアント トラフィックはネットワーク セキュリティ デバイスによって復号化されます。
Answer: B (メーッセージを残す**)**

問題は B です。Active Directory ユーザーが Netskope テナントに同期されていません。これは、ログ メッセージ 警告: ユーザーのメール ID がありません: Clarke、Daxmeifield、DC=local、使用をスキップします」から明らかです。これは、ユーザー Clarke が Active Directory に有効なメール アドレスを持っていないことを意味します。これは Netskope クライアントが動作するために必要です。Netskope クライアントは、ユーザーのメール アドレスを使用してクライアントを認証し、有効にします。したがって、オプション B は正しく、他のオプションは正しくありません。

最新問題: **24**
顧客は、Netskope を使用して、PCI データが企業認可の OneDrive インスタンスから流出するのを防止したいと考えています。このシナリオでは、どの 2 つのソリューションがデータの流出防止に役立ちますか? (2 つ選択してください。)
A. API データ保護
B. クラウド ファイアウォール (CFW)
C. SaaS セキュリティ態勢管理 (SSPM)
D. リアルタイム保護
Answer: A,D (メーッセージを残す**)**
説明
PCI データが企業認可の OneDrive インスタンスから出ないようにするために、顧客は API データ保護とリアルタイム保護を使用できます。API データ保護は、OneDrive などのクラウド サービスに既に存在するデータを検出、分類、保護できる機能です。ユーザー、コンテンツ、アクティビティ、DLP プロファイルなどの基準に基づいて、PCI データに一致するポリシーを作成できます。次に、外部の共同作業者の削除、パブリック リンクの削除、検疫など、PCI データの共有や流出を防ぐためのアクションを選択できます3。リアルタイム保護は、ユーザーと OneDrive などのクラウド サービス間で転送中のデータを検査および制御できる機能です。ユーザー、デバイス、場所、カテゴリ、DLP プロファイルなどの基準に基づいて、PCI データに一致するポリシーを作成できます。次に、ブロック、アラート、暗号化、透かしなど、PCI データのアップロードやダウンロードを防ぐためのアクションを選択できます4。したがって、オプション A と D は正しく、他のオプションは正しくありません。参考資料: API データ保護 - Netskope ナレッジ ポータル、リアルタイム保護 - Netskope ナレッジ ポータル

最新問題: **25**
展示品をレビューします。

Exhibit

```
[MVCCPDU:2021-11-02 09:02:39.742 -06:00] sslhelper.cpp:77:verify_callback():0x0
Error verifying certificate at depth 2 error self signed certificate in
certificate chain
```


NPA 接続の問題を診断しているときに、Netskope クライアント ログにエラー メッセージが表示されます。
展示物を参照すると、このエラーは何を表していますか?
A. Netskope クライアントは別のデータセンターに負荷分散されました。
B. プライマリ発行者が利用できないか、アクセスできません。
C. EDNS または LDNS 解決エラーがあります。
D. NPA TLS 接続を傍受しようとしているアップストリーム デバイスが存在します。
Answer: D (メーッセージを残す**)**
展示のエラー メッセージは、上流デバイスが NPA TLS 接続を傍受しようとしていることを示しています。エラー メッセージは、「ERROR SSL certificate validation failed: self signed certificate in certificate chain」です。これは、Netskope クライアントが、Netskope ではなく、クライアントと Netskope クラウド間のトラフィックを傍受して復号化しているデバイスによって発行された証明書を受信していることを意味します。これにより、クライアントが NPA サービスへの安全な接続を確立できず、プライベート アプリケーションにアクセスできなくなる可能性があります4。この問題を解決するには、ファイアウォールやプロキシなど、SSL 復号化を実行している上流デバイスをバイパスするか信頼する必要があります5。したがって、オプション D は正しく、他のオプションは正しくありません。参考資料: Netskope クライアントのトラブルシューティング - Netskope Knowledge Portal、Netskope クライアントのトラブルシューティング ガイド - The Netskope Community

最新問題**: 26**

顧客は、すべての Web トラフィックを保護するために Netskope Secure Web Gateway を実装しています。特定のカテゴリをブロックするポリシーは作成されていますが、まだ分類されていない新しいサイトが毎日多数あります。顧客のユーザーは迅速なアクセスを必要としており、ポリシーの変更を必要とするアクセスのリクエストやサイトのカテゴリの変更を待つことはできません。
この問題を解決するために、これらの種類のサイトへの迅速かつ安全なアクセスを提供する Netskope の機能はどれですか?
A. Netskope クラウド ファイアウォール (CFW)
B. Netskope リモート ブラウザ分離 (RBI)
C. Netskope 継続的セキュリティ評価 (CSA)
D. Netskope SaaS セキュリティ ポスチャ管理 (SSPM)
Answer: (解答を表示する**)**
分類されていない危険な Web サイトへの迅速かつ安全なアクセスを提供するという問題を解決するために、お客様が使用すべき Netskope 機能は、Netskope Remote Browser Isolation (RBI) です。Netskope RBI は、Netskope Secure Web Gateway サービスの一部であり、Web サイトへのユーザーのブラウジング セッションを傍受し、そのユーザーのコンテンツを取得して、分離されたブラウジング インスタンスでコンテンツをレンダリングするプロキシとして機能します。レンダリングされたコンテンツは、安全なピクセル ストリームとしてユーザーのブラウザーに配信されます。これにより、エンド ユーザーのデバイスとエンタープライズ ネットワークおよびシステムが安全にサイロ化され、ブラウジング アクティビティから分離され、攻撃者が制御を確立したり、他のシステムに侵入してデータを盗み出す能力が制限されます1。Netskope RBI は、Netskope Security Cloud 内の 「分離」ポリシー アクションを使用して、任意の Web サイト カテゴリまたはドメインに対して簡単に呼び出すことができます2。したがって、オプション B が正解であり、他のオプションは不正解です。参考資料: リモート ブラウザ分離 - Netskope ナレッジ ポータル、Netskope リモート ブラウザ分離 - Netskope

最新問題**: 27**
あるエンジニアリング会社は、Netskope DLP を使用して、回路図や図面などの機密文書を識別してブロックしています。最近、これらの文書がブロックされると、特定の従業員がスクリーンショットを撮ってアップロードする可能性があることが判明しました。同社は、スクリーンショットのアップロードをブロックしたいと考えています。
この要件を満たすにはどの機能を使用しますか?
A. 完全データー致 (EDM)
B. 文書フィンガープリンティング
C. ML画像分類器
D. 光学文字認識 (OCR)
Answer: C (メーッセージを残す**)**
説明
スクリーンショットがアップロードされないようにするには、エンジニアリング会社は Netskope DLP の ML 画像分類機能を使用する必要があります。この機能は、機械学習を使用して、スクリーンショット、ホワイトボード、パスポート、運転免許証などの画像内の機密情報を検出します。会社は、スクリーンショット分類に一致する画像のアップロードをブロックする DLP ポリシーを作成できます。これにより、従業員が機密文書のスクリーンショットを撮って DLP 制御を回避することを防ぐことができます。参考資料: 改良された DLP 画像分類、Netskope データ損失防止、機械学習ベースのソース コード分類の重要性

最新問題**: 28**

ある市では、許可申請書など、さまざまなフォームを使用しています。これらのフォームには、市民の個人情報や財務情報が含まれています。リモートの従業員はこれらのフォームをダウンロードし、市民と直接協力してフォームに記入します。市は、特定のフォームを識別して監視し、従業員が記入済みのフォームをダウンロードできないようにしたいと考えています。
このタスクを実行するにはどの機能を使用しますか?
A. 完全データー致 (EDM)
B. 正規表現 (regex)
C. 文書フィンガープリンティング
D. 光学文字認識 (OCR)
Answer: (解答を表示する**)**
市が使用する特定のフォームを識別して監視し、職員が記入済みのフォームをダウンロードできないようにするには、ドキュメント フィンガープリンティングを使用する必要があります。ドキュメント フィンガープリンティングは、ドキュメントの内容と構造に基づいてドキュメントに固有の署名を作成できる機能です。この署名を使用して、元のドキュメントと類似または同一の他のドキュメントを照合できます3。サンプル ドキュメントをアップロードするか、クラウド サービスから 1 つ選択することで、Netskope でドキュメント フィンガープリンティング プロファイルを作成できます4。その後、データ保護ポリシーでこのプロファイルを使用して、フィンガープリントに一致するドキュメントにブロック、アラート、検疫などのアクションを適用できます5。したがって、オプション C は正しく、他のオプションは間違っています。参考資料: ドキュメント フィンガープリンティング - Netskope Knowledge Portal、ドキュメント フィンガープリンティング プロファイルの作成 - Netskope Knowledge Portal、データ保護のポリシーの追加 - Netskope Knowledge Portal

最新問題: **29**
特権ユーザー向けのテナント アクセス セキュリティとガバナンス制御を実装しています。Netskope Cloud Security Platform 内でネイティブに利用可能で、外部またはサードパーティの統合を必要としない制御から始める必要があります。
このシナリオでは、どの 3 つのアクセス制御を使用しますか? (3 つ選択してください。)
A. 送信元 IP アドレスに基づいてアクセスを制御するための IP 許可リスト。
B. 管理者ユーザーが UI からロックアウトされるまでの失敗試行回数を設定するログイン試行。
C. 事前定義されたロールまたはカスタム ロールを適用して、管理者のアクセスをその職務に必要な機能のみに制限します。
D. ユーザーの信頼性を検証するための多要素認証。
E. 過去のセキュリティアクションに基づく履歴ベースのアクセス制御。
Answer: A,B,C (メーッセージを残す**)**
特権ユーザーに対するテナント アクセス セキュリティとガバナンス制御を実装するには、Netskope Cloud Security Platform 内でネイティブに利用可能で、外部またはサードパーティの統合を必要としない次のアクセス制御を使用できます。
* ソース IP アドレスに基づいてアクセスを制御する IP 許可リスト。これにより、Netskope テナント 2 へのアクセスを許可する IP アドレスを指定できます。これにより、不明または悪意のあるソースからの不正アクセスを防ぐことができます。
* ログイン試行回数を設定して、管理者ユーザーが UI からロックアウトされるまでの失敗回数を設定します。これにより、管理者が間違ったパスワードを入力できる回数を設定でき、その後は指定された期間ロックアウトされます3。これにより、ブルートフォース攻撃やパスワード推測の試みを防ぐことができます。
* 定義済みまたはカスタムのロールを適用して、管理者のアクセスをその職務に必要な機能のみに制限します。これにより、ロールと責任に基づいて、さまざまな管理者にさまざまなレベルの権限とアクセス権を割り当てることができます4。これにより、最小権限の原則を強制し、管理者権限の誤用や乱用のリスクを軽減できます。したがって、オプション A、B、C は正しく、その他のオプションは

間違っています。参考資料: 安全なテナント構成と強化 - Netskope Knowledge Portal、管理者設定 - Netskope Knowledge Portal、ロールの作成 - Netskope Knowledge Portal

最新問題: **30**
会社では、DLP ポリシーによってトリガーされた隔離されたファイルを保持する必要があります。このシナリオでは、どのステートメントが正しいですか?
A. ファイルは、隔離プロファイルに割り当てられたデータ センターにリモートで保存されます。
B. ファイルは、検疫プロファイルで割り当てられた Netskope データセンターに保存されます。
C. ファイルは、検疫プロファイルに割り当てられたクラウド プロバイダーに保存されます。
D. ファイルは、検疫プロファイルに割り当てられた管理者コンソール PC に保存されます。
Answer: B (メーッセージを残す**)**
説明
ポリシーによって隔離対象としてファイルにフラグが付けられると、そのファイルは隔離フォルダに配置され、代わりに元の場所にトゥームストーン ファイルが配置されます。隔離フォルダは、隔離プロファイルで割り当てられた Netskope データ センターにあります。隔離プロファイルは、[設定] > [脅威保護] > [API 対応保護] で構成します。隔離されたファイルは、ユーザーが誤ってファイルをダウンロードするのを防ぐために、圧縮され、パスワードで保護されます。その後、Netskope はプロファイル 1 で指定された管理者に通知します。したがって、オプション B が正しく、他のオプションは正しくありません。参照: 隔離 - Netskope ナレッジ ポータル、脅威保護 - Netskope ナレッジ ポータル

最新問題: **31**
Netskope テナントにユーザーとグループをプロビジョニングしたいと考えています。2 つの異なるフォレストにホストされている Microsoft Active Directory サーバーがあります。このシナリオについて正しい記述はどれですか。
A. ユーザープロビジョニングには Netskope アダプター ツールを使用できます。
B. ユーザープロビジョニングにはNetskope仮想アプライアンスを使用できます
C. Azure AD または Okta に移行するまで、ユーザーをプロビジョニングすることはできません。
D. ユーザープロビジョニングには SCIM バージョン 2 を使用できます。
Answer: D (メーッセージを残す**)**
説明
このシナリオでは、ユーザー プロビジョニングに SCIM バージョン 2 を使用できます。SCIM (System for Cross-domain Identity Management) は、異なるクラウド アプリケーション間で ID 情報を交換するための標準プロトコルです。
Netskope は SCIM バージョン 2 をサポートしており、Microsoft Azure AD、Okta、OneLogin、Ping Identity など、同じ標準に従う ID プロバイダー (IdP) と統合できます。SCIM を使用して、複数の Active Directory フォレストから Netskope テナントにユーザーとグループをプロビジョニングできます。他のオプションはこのシナリオでは無効です。Netskope アダプター ツールと Netskope 仮想アプライアンスは、プロビジョニングではなく、ユーザー識別に使用されます。一度に 1 つの Active Directory フォレストにのみ接続できます。Netskope は SCIM を使用する他の IdP もサポートしているため、ユーザーをプロビジョニングするために Azure AD または Okta に移行する必要はありません。参照: Netskope クライアントのユーザーのプロビジョニング1、SCIM 統合2

最新問題: **32**
IT 組織では、ユーザー ディレクトリ サービスを Microsoft Active Directory からクラウドベースの ID プロバイダー (IdP) ソリューションである Azure AD に移行しています。この新しいクラウドベースの IdP で動作するように、Netskope ユーザー プロビジョニング プロセスを調整することが求められています。
A. 手動インポート
B. Microsoft GPO
C. ディレクトリインポーター
D. SCIMアプリ
Answer: (解答を表示する**)**

最新問題: **33**
顧客データベースのコンテンツが Dropbox にアップロードされたときにのみポリシーをトリガーすることで、誤検知を減らしたいと考えています。データベースの最大サイズは 2 MB です。このシナリオでは、このタスクを実行する 2 つの方法は何ですか? (2 つ選択してください。)
A. .csv エクスポートを Netskope テナント DLP ルール セクションにアップロードして、完全一致ハッシュを作成します。
B. Netskope クライアントを使用して、.csv エクスポートを Netskope 管理プレーン DLP コンテナーにアップロードします。
C. 件名を 完全一致ハッシュの作成」として、サポート チケットを使用して .csv エクスポートを Netskope に送信します。
D. Netskope 仮想アプライアンスを使用して、完全一致ハッシュを作成します。
Answer: (解答を表示する**)**
顧客データベースの内容が Dropbox にアップロードされたときにのみポリシーをトリガーすることで誤検知を減らすには、次の 2 つの方法を使用できます。.csv エクスポートを Netskope テナントの DLP ルール セクションにアップロードして、完全一致ハッシュを作成します。これは、顧客データベースなどの構造化データを含むファイルを Netskope テナントにアップロードし、データのハッシュを生成する方法です。次に、このハッシュを使用してクラウド トラフィック内のデータが照合され、DLP ポリシーがトリガーされます。この方法は、サイズが 10 MB 未満のファイルに適しています。ファイルをアップロードするには、[ポリシー] > [データ保護] > [DLP ルール] に移動し、[完全一致ハッシュ] をクリックする必要があります。次に、ローカル システムからファイルを選択してアップロードします。Netskope 仮想アプライアンスを使用して完全一致ハッシュを作成します。これは、顧客データベースなどの構造化データを含むファイルを作成し、仮想アプライアンスを使用して Netskope クラウドにアップロードする方法です。仮想アプライアンスは、ファイルをアップロードする前に暗号化し、データのハッシュを生成します。その後、ハッシュを使用してクラウド トラフィック内のデータが照合され、DLP ポリシーがトリガーされます。この方法は、サイズが 10 MB を超えるファイルに適しています。ファイルを作成するには、特定の形式に従って .csv ファイルとして保存する必要があります。ファイルをアップロードするには、仮想アプライアンス CLI で request dlp-pdd upload コマンドを使用する必要があります。その他のオプションは、このタスクには有効な方法ではありません。Netskope クライアントを使用して .csv エクスポートを Netskope 管理プレーン DLP コンテナーにアップロードすることはできません。これはクライアントでサポートされている機能ではないためです。件名が 完全一致ハッシュの作成」のサポート チ

ケットを使用して .csv エクスポートを Netskope に送信することはできません。これは、完全一致ハッシュを作成する安全で効率的な方法ではないためです。参考資料: UI からの完全一致ハッシュの作成1、仮想アプライアンスからの完全一致ハッシュの作成2

最新問題**: 34**
Netskope DLP ソリューションを使用しています。クレジットカードのテスト データを含むファイルを Dropbox にアップロードしても、DLP イベントがトリガーされないことに気付きました。対応するページ イベントがあります。この動作の原因となるシナリオは 2 つありますか? (2 つ選択してください。)
A. Netskope クライアントは Dropbox トラフィックを誘導していません。
B. DLP ルールの重大度しきい値が発生回数よりも高い値に設定されています。
C. テスト データ内のクレジットカード番号は無効な 16 桁の番号です。
D. Dropbox に API 保護が設定されていません。
Answer: B,C (メーッセージを残す**)**
説明
クレジットカードのテスト データを含むファイルを Dropbox にアップロードしたときに、DLP イベントがトリガーされない原因となるシナリオは 2 つ考えられます。1 つは、DLP ルールの重大度しきい値が発生回数よりも高い値に設定されていることです。つまり、機密データに一致する回数が指定されたしきい値を超えた場合にのみ、ルールによってイベントがトリガーされます。たとえば、ルールの重大度しきい値が 10 で、ファイルにクレジットカード番号が 5 つしか含まれていない場合、イベントは生成されません。これを修正するには、重大度しきい値を下げるか、しきい値を完全に削除します。もう 1 つのシナリオは、テスト データ内のクレジットカード番号が無効な 16 桁の数字である場合です。つまり、その番号は、Netskope DLP が有効なクレジットカード番号を検出するために使用する検証方法である Luhn アルゴリズム チェックに合格しません。たとえば、番号が 1234-5678-9012-3456 の場合、有効なクレジットカード番号ではないため、Netskope DLP では検出されません。これを修正するには、Luhn アルゴリズム チェックに合格した有効なテスト クレジットカード番号を使用できます。その他のオプションは、この動作の有効なシナリオではありません。Netskope クライアントが Dropbox トラフィックを誘導していないのは、対応するページ イベントがあるため有効なシナリオではありません。つまり、トラフィックは Netskope に誘導されています。Dropbox に API 保護が設定されていないのは、ファイル アップロード時の DLP 検出には API 保護が必要ないため有効なシナリオではありません。ファイル アップロード時の DLP 検出はリアルタイム保護によって処理されます。参照: DLP ルール設定 1、クレジットカード番号検出 2

最新問題**: 35**
あるエンジニアリング会社は、Netskope DLP を使用して、回路図や図面などの機密文書を識別してブロックしています。最近、これらの文書がブロックされると、特定の従業員がスクリーンショットを撮ってアップロードする可能性があることが判明しました。同社は、スクリーンショットのアップロードをブロックしたいと考えています。
この要件を満たすにはどの機能を使用しますか?
A. 完全データー致 (EDM)
B. 文書フィンガープリンティング
C. ML画像分類器
D. 光学文字認識 (OCR)
Answer: C (メーッセージを残す**)**
スクリーンショットがアップロードされないようにするには、エンジニアリング会社は Netskope DLP の ML 画像分類機能を使用する必要があります。この機能は、機械学習を使用して、スクリーンショット、ホワイトボード、パスポート、運転免許証などの画像内の

機密情報を検出します。会社は、スクリーンショット分類に一致する画像のアップロードをブロックする DLP ポリシーを作成できます。これにより、従業員が機密文書のスクリーンショットを撮って DLP 制御を回避することを防ぐことができます。参考資料: 改良された DLP 画像分類、Netskope データ損失防止、機械学習ベースのソース コード分類の重要性

最新問題**: 36**
展示品をレビューします。

スポーツとしてタグ付けされた YouTube コンテンツへのユーザーのアクセスを制限するように求められています。必要なリアルタイム ポリシーを作成しましたが、ユーザーは引き続きコンテンツにアクセスできます。図を参照すると、何が問題なのでしょうか。
A. ウェブサイトはステアリング ポリシー例外状態です。
B. ポリシーの変更は適用されていません。
C. YouTube コンテンツを制御できません。
D. トラフィックがDo Not Decryptポリシーに一致しました
Answer: D (メーッセージを残す**)**
このシナリオの問題は、トラフィックがDo Not Decryptポリシーに一致したことです。Do Not Decryptポリシーは、トラフィックを暗号化したままにして、NetskopeのReal-time Protectionポリシー1を介してそれ以上分析しないように指定するルールです。図では、ユーザーからYouTubeへのトラフィックに

「トラフィックのバイパス」の値が「はい」で、「Netskope」の値が「はい」です。これは、トラフィックが Netskope に誘導されたが、復号化も検査もされていないことを意味します2。したがって、スポーツとしてタグ付けされた YouTube コンテンツへのユーザーのアクセスを制限するために作成されたリアルタイム ポリシーは適用されず、ユーザーは引き続きコンテンツにアクセスできます。この問題を解決するには、YouTube へのトラフィックに一致する「復号化しない」ポリシーを削除または変更するか、ポリシーでスポーツ カテゴリの例外を作成する必要があります3。したがって、オプション D は正しく、他のオプションは正しくありません。参考資料: ページ イベント - Netskope Knowledge Portal、SSL 復号化のポリシーの追加 - Netskope Knowledge Portal、YouTube コンテンツ コントロール - Netskope Knowledge Portal

最新問題: **37**
展示品をレビューします。

セキュリティ アナリストは、過去 90 日間にアクセスされた未承認アプリケーションの上位 5 つのカテゴリを表示するレポートを作成する必要があります。図を参照すると、このレポートを作成するために使用される Advanced Analytics のデータ コレクションは 2 つありますか (2 つ選択してください)。

A. アラート
B. アプリケーションイベント
C. ページイベント
D. ネットワークイベント

Answer: B,D (メーッセージを残す**)**

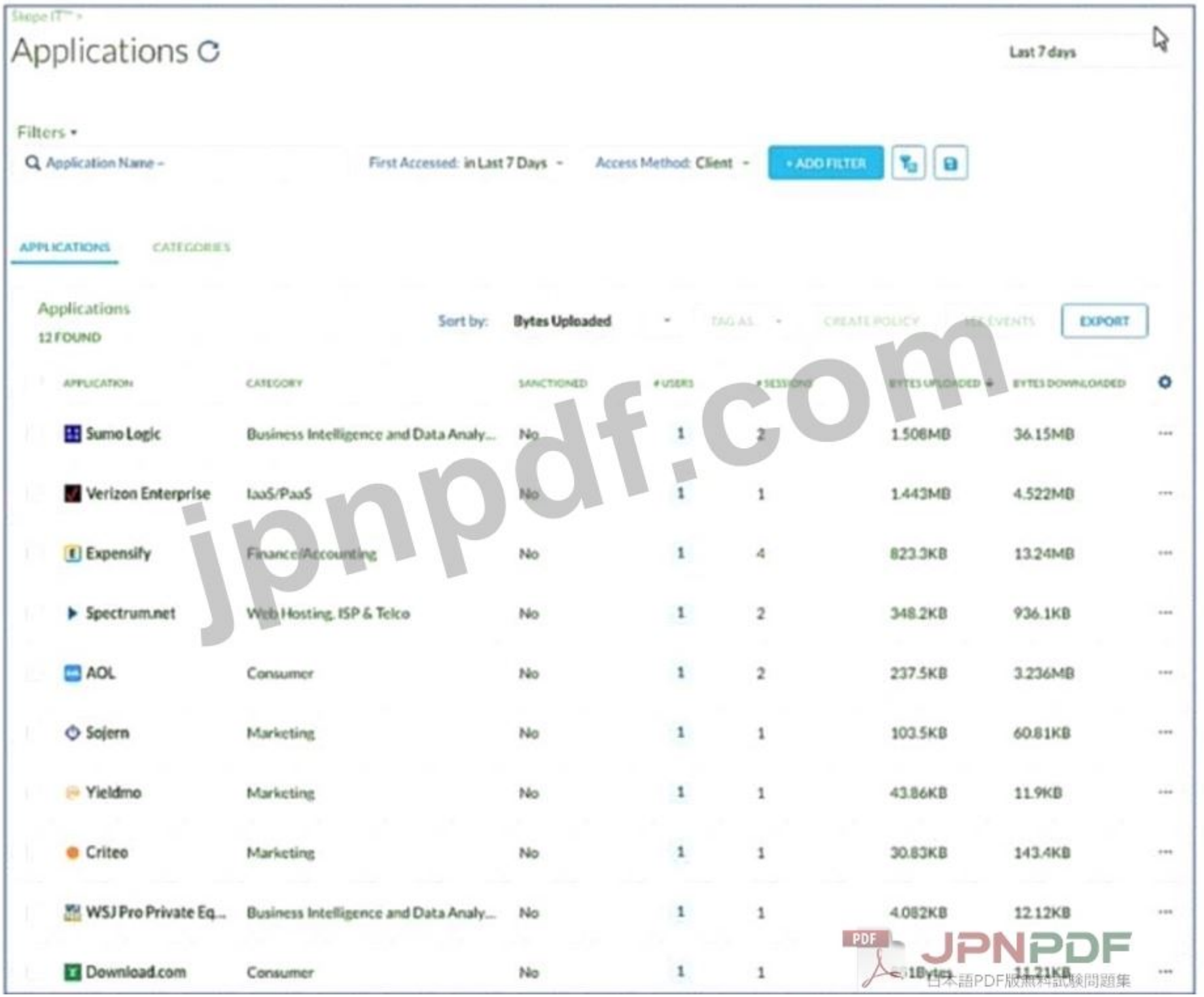
過去 90 日間にアクセスされた未承認アプリケーションの上位 5 つのカテゴリを表示するレポートを作成するには、セキュリティ アナリストは、Advanced Analytics のアプリケーション イベントとネットワーク イベントという 2 つのデータ コレクションを使用する必要があります。アプリケーション イベントは、アプリ名、アプリ カテゴリ、アプリのリスク スコア、アプリ インスタンス、アプリ バージョンなど、ユーザーがアクセスしたクラウド アプリケーションと Web サイトに関する情報を提供します。ネットワーク イベントは、ソース IP、宛先 IP、プロトコル、ポート、送信バイト数、受信バイト数など、ユーザーが生成したネットワーク トラフィックに関する情報を提供します。これら 2 つのデータ コレクションを組み合わせることで、セキュリティ アナリストは、アプリ カテゴリ、

アプリのリスク スコア、時間範囲でイベントをフィルター処理し、過去 90 日間にアクセスされた未承認アプリケーションの上位 5 つのカテゴリを示すレポートを作成できます。アラートとページ イベントはこのレポートには関係ありません。アラートは、アラートの種類、アラートの重大度、アラートのステータス、アラートの説明など、リアルタイム保護または API データ保護ポリシーによってトリガーされたアラートに関する情報を提供します。ページ イベントは、ページ タイトル、ページ URL、ページ カテゴリ、ページ リスク スコア、ページ コンテンツ タイプなど、ユーザーがアクセスした Web ページに関する情報を提供します。参考資料: 高度な分析

最新問題**: 38**
Netskope プラットフォームにユーザー ID とグループの両方をインポートできるようにしたいと考えています。この要件を満たす 2 つの方法はどれですか? (2 つ選択してください。)
A. クロスドメイン ID 管理 (SCIM) 用のシステムを使用します。
B. 手動入力を使用します。
C. ディレクトリインポーターを使用します。
D. CSV ファイルで一括アップロードを使用します。
Answer: A,D (メーッセージを残す**)**
説明
Netskope プラットフォームにユーザー ID とグループの両方をインポートできるようにするには、System for Cross-domain Identity Management (SCIM) 方式または CSV ファイルによる一括アップロード方式のいずれかを使用できます。
どちらの方法でも、SCIM または CSV 形式をサポートするさまざまな ID プロバイダー (IdP) からユーザー ID とグループをインポートできます。SCIM 方法は、ユーザー プロビジョニングのためにアプリ間でユーザー ID 情報の交換を自動化するため、大規模な展開に推奨されます。CSV 方法は、カンマ区切り値ファイルでユーザーの詳細を手動でアップロードできるため、小規模な展開に推奨されます。その他の方法はこの要件には適していません。手動エントリ方法では、グループのインポートはできず、ユーザーのメール アドレスのみをインポートできます。ディレクトリ インポーター方法では、ユーザーとグループを Netskope プラットフォームに直接インポートするのではなく、Active Directory または LDAP サーバーに接続して、ユーザーとグループの情報を定期的に取得します。
参考資料: Netskope クライアントのユーザーのプロビジョニング2、SCIM 統合3、CSV ファイルによる一括アップロード

最新問題**: 39**
展示品をレビューします。

Exhibit



組織内で使用されている新しいクラウド アプリケーションを検出したいと考えています。
展示物を参照すると、どの 3 つの方法がこのタスクを達成しますか? (3 つ選択してください。)

A. SaaS アプリケーション用の API 対応の保護インスタンスを設定します。
B. オンプレミス ログ パーサー (OPLP) をデプロイします。
C. フォワードプロキシステアリング方式を使用してクラウドトラフィックをNetskopeに誘導する
D. Netskope UI の Cloud Confidence Index (CCI) 内の 「すべてのアプリ」を表示します。

E. ファイアウォールまたはプロキシのログを Netskope プラットフォームに直接アップロードします。
Answer: B,C,E (メーッセージを残す**)**
説明
組織内で使用されている新しいクラウド アプリケーションを検出するには、B. オンプレミス ログ パーサー (OPLP) を展開する、C. フォワード プロキシ ステアリング メソッドを使用してクラウド トラフィックを Netskope に誘導する、E. ファイアウォールまたはプロキシ ログを Netskope プラットフォームに直接アップロードする、という 3 つの方法があります。オンプレミス ログ パーサー (OPLP) は、オンプレミスのファイアウォールまたはプロキシ デバイスからのログを解析し、分析とレポートのために Netskope クラウドに送信できるソフトウェア コンポーネントです。ネットワーク内の Linux サーバーに OPLP を展開し、ログ ソースに接続してログを定期的またはリアルタイムでアップロードするように構成できます3。フォワード プロキシ ステアリング メソッドは、ユーザーのデバイスまたはブラウザーから Netskope クラウドに Web トラフィックを誘導して、検査とポリシーの適用を行う方法です。PAC ファイル、VPN、インライン プロキシなどのフォワード プロキシ ステアリング メソッドを使用して、トラフィックを Netskope に誘導し、使用されている新しいクラウド アプリケーションを検出できます4。ファイアウォールまたはプロキシ ログを Netskope プラットフォームに直接アップロードすることは、ログ ソースから Netskope クラウドにログを手動で送信して分析とレポートを行う方法です。ファイアウォールまたはプロキシ ログを Netskope プラットフォームに直接アップロードするには、[SkopeIT] > [設定] > [ログのアップロード] > [新しいログのアップロード] に移動し、ログ ソースの種類、ファイル形式、ログ ファイル、およびタイム ゾーンを選択します5。したがって、オプション B、C、および E は正しく、その他のオプションは正しくありません。参考資料: オンプレミス ログ パーサー - Netskope Knowledge Portal、トラフィック ステアリング - Netskope Knowledge Portal、ファイアウォールまたはプロキシ ログをプラットフォームに直接アップロード - Netskope Knowledge Portal

最新問題**: 40**
Netskope DLP ソリューションを使用しています。クレジットカードのテスト データを含むファイルを Dropbox にアップロードしても、DLP イベントがトリガーされないことに気付きました。対応するページ イベントがあります。この動作の原因となるシナリオは 2 つありますか? (2 つ選択してください。)
A. Netskope クライアントは Dropbox トラフィックを誘導していません。
B. DLP ルールの重大度しきい値が発生回数よりも高い値に設定されています。
C. テスト データ内のクレジットカード番号は無効な 16 桁の番号です。
D. Dropbox に API 保護が設定されていません。
Answer: (解答を表示する**)**
クレジットカードのテスト データを含むファイルを Dropbox にアップロードしたときに、DLP イベントがトリガーされない原因となるシナリオは 2 つ考えられます。1 つは、DLP ルールの重大度しきい値が発生回数よりも高い値に設定されていることです。つまり、機密データに一致する回数が指定されたしきい値を超えた場合にのみ、ルールによってイベントがトリガーされます。たとえば、ルールの重大度しきい値が 10 で、ファイルにクレジットカード番号が 5 つしか含まれていない場合、イベントは生成されません。これを修正するには、重大度しきい値を下げるか、しきい値を完全に削除します。もう 1 つのシナリオは、テスト データ内のクレジットカード番号が無効な 16 桁の数字である場合です。つまり、その番号は、Netskope DLP が有効なクレジットカード番号を検出するために使用する検証方法である Luhn アルゴリズム チェックに合格しません。たとえば、番号が 1234-5678-9012-3456 の場合、有効なクレジットカード番号ではないため、Netskope DLP では検出されません。これを修正するには、Luhn アルゴリズム チェックに合格した有効なテスト クレジットカード番号を使用できます。その他のオプションは、この動作の有効なシナリオではありません。Netskope クライアントが Dropbox トラフィックを誘導していないのは、対応するページ イベントがあるため有効なシナリオではありません。つまり、トラフィックは Netskope に誘導されています。Dropbox に API 保護が設定されていないのは、ファイル アップロード時の

DLP 検出には API 保護が必要ないため有効なシナリオではありません。ファイル アップロード時の DLP 検出はリアルタイム保護によって処理されます。参照: DLP ルール設定 1、クレジットカード番号検出 2

最新問題: **41**
顧客は現在、Netskope クライアントで SSO を使用してのみ、ユーザーに OneDrive の企業インスタンスへのアクセスを許可しています。ユーザーは休暇中にラップトップを持ち出すことはできませんが、緊急の要求があった場合は OneDrive 上のドキュメントにアクセスする必要があることがあります。顧客は、管理されていないデバイスから従業員が OneDrive にリモート アクセスできるようにしながら、DLP コントロールを適用して機密ファイルを管理されていないデバイスにダウンロードすることを禁止したいと考えています。
このシナリオの要件を満たすステアリング方法はどれでしょうか?
A. SSO と統合されたリバース プロキシを使用します。
B. SSO と統合されたクラウド サービス プロバイダーとのプロキシ チェーンを使用します。
C. SSO と統合されたフォワード プロキシを使用します。
D. オンプレミス プロキシと統合された安全なフォワーダーを使用します。
Answer: A (メーッセージを残す)
説明
SSO と統合されたリバース プロキシは、このシナリオの要件を満たします。リバース プロキシは、ユーザーからクラウド アプリへの要求をインターセプトし、ユーザー ID、デバイスの状態、アプリ、およびデータ コンテキストに基づいてポリシーを適用します。DLP コントロールを適用して、管理されていないデバイスへの機密ファイルのダウンロードを禁止できます。また、顧客の SSO プロバイダーと統合して、ユーザーを認証し、OneDrive の企業インスタンスへのアクセスのみを許可することもできます。その他のステアリング方法は、Netskope クライアントを必要とするか、クラウド アプリのアクティビティを細かく制御できないため、このシナリオには適していません。

最新問題: **42**
SCIM プロビジョニングを使用して Okta から Netskope ユーザーをプロビジョニングしていますが、ユーザーがテナントに表示されません。このシナリオでは、正確性を確認するために、まず Okta でどの 2 つの Netskope コンポーネントを検証する必要がありますか?
（2つ選択してください。）
A. IdP エンティティ ID
B. OAuthトークン
C. Netskope SAML証明書
D. SCIM サーバー URL
Answer: B,D (メーッセージを残す)
説明
SCIM プロビジョニングを使用して Okta から Netskope ユーザーをプロビジョニングし、ユーザーがテナントに表示されない場合は、正確性を確認するために最初に Okta で検証する必要がある 2 つの Netskope コンポーネントは、B. OAuth トークンと D. です。SCIM サーバー URL。OAuth トークンは、Okta が Netskope SCIM サーバーで認証し、ユーザー プロビジョニング操作を実行できるようにする認証情報です4。SCIM サーバー URL は、Okta が Netskope SCIM サーバーと通信してユーザー データを送信するために使用するエンドポイントです5。SCIM プロビジョニングが機能するには、これらのコンポーネントの両方が Okta で正しく構成されている

必要があります。これらは、Netskope UI の [設定] > [ツール] > [ディレクトリ ツール] > [SCIM 統合] にあります6。したがって、オプション B と D は正しく、その他のオプションは間違っています。参考資料: SCIM ベースのユーザー プロビジョニング - Netskope Knowledge Portal、Netskope + Okta ユース ケース: SCIM を使用したユーザーのプロビジョニングとグループの管理 - Netskope、Netskope パートナー Okta - Netskope

最新問題: **43**
Netskope のファイルハッシュ リストの目的は何ですか?
A. カスタム マルウェア検出プロファイルで参照されるブロックリストと許可リストのエントリを構成します。
B. Netskope が検査できるファイルの種類を提供します。
C. URL を許可またはブロックするために使用されます。
D. クライアント脅威エクスプロイト防止 (CTEP) を提供します。
Answer: A (メーッセージを残す**)**
説明
Netskope のファイル ハッシュ リストの目的は、カスタム マルウェア検出プロファイルで参照されるブロック リストと許可リストのエントリを構成することです。ファイル ハッシュ リストは、組織内で許可またはブロックするファイルを表す MD5 または SHA-256 ハッシュのコレクションです。ファイル プロファイルを追加するときにファイル ハッシュ リストを作成し、組織内のファイルの許可リストまたはブロック リストとして使用できます1。その後、マルウェア検出プロファイルを作成するときにファイル ハッシュ リストを選択できます2。

最新問題: **44**
DevSecOps エンジニアが REST API v2 を使用して URL リストを作成および更新できるようにするために、API トークンを作成しています。このシナリオでは、API トークンにどの権限を作成する必要がありますか?
A. 「events」エンドポイントへの読み取りおよび書き込みアクセスを提供します。
B. 「urllist」エンドポイントに読み取りおよび書き込みアクセスを提供します。
C. 「urllist」エンドポイントに読み取りアクセスのみを提供します。
D. 「urllist」エンドポイントに書き込みアクセスのみを提供します。
Answer: (解答を表示する**)**
説明
DevSecOpsエンジニアがREST API v2を使用してURLリストを作成および更新できるようにAPIトークンを作成するには、「urllist」エンドポイントに読み取りおよび書き込みアクセスを提供する必要があります。「urllist」エンドポイントは、Netskopeテナント内のURLリストを管理できるAPIエンドポイントです。このエンドポイントを使用して、URLリストの作成、更新、削除、リストなどの操作を実行できます3。この権限でAPIトークンを作成するには、[設定] > [ツール] > [REST API v2] > [新しいトークン]に移動し、トークン名と有効期限を入力し、
「urllist」エンドポイントにアクセスし、権限として 「読み取り+書き込み」を選択します4。これにより、DevSecOps エンジニアはリクエストで API トークンを使用して URL リストを作成および更新できるようになります。したがって、オプション B は正しく、他のオプションは誤りです。参考資料: REST API v2 の概要 - Netskope Knowledge Portal、URL リストの管理 - Netskope Knowledge Portal

最新問題: **45**

Netskope クライアント アイコンに赤い点があり、アイコンの上にマウスを移動すると 「エラーのため無効」と表示されます。このメッセージが表示される 2 つの理由は何ですか? (2 つ選択してください。)
A. クライアント サービスは手動で停止されます。
B. ステアリング例外が正しくありません。
C. クライアントのヘルスチェックに失敗しました。
D. クライアント トラフィックは iPsec 経由で送信されます。
Answer: A,C (メーッセージを残す)
Netskope クライアント アイコンにマウスを合わせたときに 「エラーのため無効」というメッセージが表示される理由は、A. クライアント サービスが手動で停止されていること、および C. クライアントのヘルス チェックが失敗していることの 2 つです。クライアント サービスは、ユーザーのデバイス上で Netskope クライアントを実行し、Netskope クラウドと通信するバックグラウンド プロセスです。クライアント サービスがユーザーまたは別のプログラムによって手動で停止された場合、Netskope クライアントは無効になり、アイコンに赤い点が表示されます1。クライアントのヘルス チェックは、Netskope クライアントの状態を監視し、問題が検出された場合は自己修復アクションを実行する機能です。クライアントのヘルス チェックが失敗した場合、Netskope クライアントで、破損したファイルやレジストリ エントリなど、自動的に修復できない重大なエラーが発生したことを意味します。この場合、Netskope クライアントは無効になり、アイコンに赤い点が表示されます2。したがって、オプション A と C は正しく、他のオプションは正しくありません。参考資料: Netskope クライアントのトラブルシューティング - Netskope ナレッジ ポータル、クライアント ヘルス チェック - Netskope ナレッジ ポータル

最新問題: **46**
すべてのクラウド ストレージ アプリケーションにマルウェア保護を提供したいと考えています。
このシナリオでは、どのアクションがこのタスクを達成しますか?
A. Cloud Storage カテゴリを使用して、リアルタイム脅威保護ポリシーを作成します。
B. データ保護プロファイルを適用します。
C. CTEP プロファイルを適用します。
D. Cloud Storage カテゴリを使用して API 脅威保護ポリシーを作成します。
Answer: A (メーッセージを残す)
「クラウド ストレージ」カテゴリに特化したリアルタイムの脅威保護ポリシーを作成すると、サポートされているすべてのクラウド ストレージ アプリケーションがマルウェア保護の対象になります。このアプローチにより、クラウド ストレージ環境内でマルウェアの脅威をリアルタイムでスキャンして対応できるようになります。

最新問題: **47**

あなたの会社には、遠隔地にいて頻繁に出張するユーザーが多数います。出張中でも、ユーザーのアクティビティを最大限に把握できるようにしたいと考えています。Netskope を使用します。このシナリオではどの展開方法が使用されますか?
A. プロキシチェーンを使用します。
B. Netskope クライアントを使用します。
C. IPsec トンネルを使用します。
D. GRE トンネルを使用します。
Answer: B (メーッセージを残す**)**
リモート ユーザーや出張中のユーザーに最適な導入方法は、Netskope クライアントを使用することです。Netskope クライアントは、ユーザーのデバイス上で実行される軽量のソフトウェア エージェントで、Web トラフィックとクラウド トラフィックを Netskope クラウドに誘導して、リアルタイムの検査とポリシーの適用を行います1。Netskope クライアントは、エンド ユーザーに常時接続のリモート アクセス エクスペリエンスを提供し、パブリック クラウド環境のアプリケーションにアクセスするためにリモート ユーザーが企業ネットワークを経由するバックホール (ヘアピン) を回避します2。Netskope クライアントはオフライン モードもサポートしており、ユーザーはオフラインで作業し、インターネットに再接続したときにポリシーを同期できます。

最新問題: **48**
Google ドライブに保存されているドキュメントが公開リンクで外部に共有されるのを防ぎます。
この要件を満たすには、Netskope で何を設定しますか?
A. 脅威保護ポリシー
B. APIデータ保護ポリシー
C. リアルタイム保護ポリシー
D. 隔離
Answer: B (メーッセージを残す**)**
Google Drive に保存されているドキュメントがパブリック リンクで外部に共有されないようにするには、Netskope で API データ保護ポリシーを構成する必要があります。API データ保護ポリシーを使用すると、Google Drive1 などのクラウド サービスにすでに存在するデータを検出、分類、保護できます。ユーザー、コンテンツ、アクティビティ、DLP プロファイルなどの基準に基づいて、保護するドキュメントに一致するポリシーを作成できます。次に、外部の共同編集者の削除、パブリック リンクの削除、検疫2 など、ドキュメントが外部に共有されないようにするためのアクションを選択できます。したがって、オプション B が正しく、他のオプションは間違っています。参考資料: API データ保護 - Netskope Knowledge Portal、API データ保護のポリシーの追加 - Netskope Knowledge Portal

最新問題: **49**
顧客が AWS S3 バケット内のマルウェアを懸念しています。このシナリオに役立つ 2 つのアクションは何ですか? (2 つ選択してください。)
A. AWS インスタンスへのマルウェアのアップロードをブロックするリアルタイムポリシーを作成します。
B. すべての AWS インスタンスに対して脅威保護 (マルウェアスキャン) を有効にして、マルウェアを識別します。
C. AWS S3 バケット内のマルウェアを隔離するための API 保護ポリシーを作成します。
D. AWS S3 バケット内のマルウェアを隔離するための脅威プロファイルを作成します。
Answer: B,C (メーッセージを残す**)**
説明

AWS S3 バケットにマルウェアが存在するシナリオで顧客を支援するには、次の 2 つのアクションが役立ちます。B: すべての AWS インスタンスで脅威保護 (マルウェアスキャン) を有効にしてマルウェアを識別する、C. API 保護ポリシーを作成して AWS S3 バケット内のマルウェアを隔離する。脅威保護 (マルウェアスキャン) は、Netskope の高度な脅威保護エンジンを使用して、AWS S3 などのクラウドサービス内のファイルをマルウェアスキャンできる機能です。Netskope テナント内のすべての AWS インスタンスで脅威保護 (マルウェアスキャン) を有効にするには、[設定] > [クラウドサービス] > [AWS] > [脅威保護] に移動し、[マルウェアスキャンを有効にする] オプションを選択します1。これにより、AWS S3 バケット内のマルウェアを識別し、さらなるアクションのためにアラートを生成することができます。API 保護ポリシーは、さまざまな基準に基づいて、AWS S3 などのクラウドサービスにすでに存在するデータに Netskope が適用するアクションと通知を指定するルールです。 AWS S3 バケット内のマルウェアを隔離するための API 保護ポリシーを作成するには、[ポリシー] > [API 保護] > [新規ポリシー] に移動し、ポリシー ページ 2 で AWS サービス、マルウェア スキャン データ識別子、および隔離アクションを選択します。これにより、AWS S3 バケット内のマルウェアを隔離し、マルウェアの拡散や不正ユーザーによるアクセスを防ぐことができます。したがって、オプション B と C は正しく、その他のオプションは誤りです。参考資料: 脅威保護 (マルウェア スキャン) - Netskope Knowledge Portal、API 保護のポリシーの追加 - Netskope Knowledge Portal

最新問題**: 50**
組織には自社開発のクラウド アプリケーションがあります。ログイン、表示、ファイルのダウンロードなど、このクラウド アプリケーションでユーザーが実行するアクティビティを監視する必要があります。残念ながら、Netskope はデフォルトではこれらのアクティビティを検出できないようです。
この目標をどうやって達成しますか?
A. Netskope Private Access を使用してアプリケーションへのアクセスを有効にします。
B. クラウド アプリケーションがステアリング例外として追加されていることを確認します。
C. アプリケーションが SSL 復号化ポリシーに追加されていることを確認します。
D. Chrome 拡張機能を使用して新しいクラウド アプリケーション定義を作成します。
Answer: D (メーッセージを残す**)**
説明
自社開発のクラウド アプリケーションでユーザーが実行するアクティビティを監視するには、Chrome 拡張機能を使用して新しいクラウド アプリケーション定義を作成する必要があります。Chrome 拡張機能は、Web ベースのアプリケーションのトラフィックとアクティビティを記録し、Netskope テナント 1 にインポートできるカスタム アプリ定義を作成できるツールです。この方法では、Netskope が自社開発のクラウド アプリケーションのアクティビティを検出して分析し、それに応じてポリシーを適用できるようになります。したがって、オプション D は正解で、他のオプションは不正解です。参考資料: クラウド アプリ定義の作成 - Netskope ナレッジ ポータル

最新問題**: 51**
Netskope DLP ソリューションを使用しています。承認されていないクラウド ストレージ ソリューションにアップロードしたファイル内の有効なクレジットカード番号がポリシー違反をトリガーしていないことに気付きました。このトラフィックの Skope IT アプリケーション イベントは表示されますが、DLP アラートは表示されません。
このシナリオではどの記述が正しいでしょうか?
A. Netskope クライアントが有効になっていません。
B. 重大度しきい値をより高い値に設定しました。
C. Netskope クライアントは有効になっていますが、SaaS アプリケーションの API 保護は構成されていません。

D. クレジットカード番号は、16 桁の連続番号ではなく、スペースまたはダッシュ区切りで入力されます。
Answer: D (メーッセージを残す**)**
このシナリオで正しい記述は D です。クレジットカード番号は、16 桁の連続した数字ではなく、スペースまたはダッシュの区切り文字を使用して入力されています。これが、ファイル内の有効なクレジットカード番号が Netskope DLP によるポリシー違反をトリガーしない理由の 1 つです。Netskope DLP は、データ識別子を使用して、ファイルおよびネットワーク トラフィック内の機密データを検出します。データ識別子は、正規表現、チェックサム、キーワードなどに基づいてデータ パターンを照合する定義済みまたはカスタムのルールです1。クレジットカード番号のデータ識別子は、Luhn アルゴリズム チェックに合格する 16 桁の連続した数字と一致します2。クレジットカード番号が 1234-5678-9012-3456 や 1234 5678 9012 3456 のようにスペースまたはダッシュの区切り文字を使用して入力されている場合、データ識別子と一致しないため、ポリシー違反はトリガーされません。この問題を解決するには、クレジットカード番号から区切り文字を削除するか、区切り文字付きのクレジットカード番号と一致するカスタム データ識別子を作成します3。したがって、オプション D は正解で、他のオプションは不正解です。参考資料: データ識別子 - Netskope Knowledge Portal、クレジットカード番号 - Netskope Knowledge Portal、カスタム データ識別子の作成 - Netskope Knowledge Portal

最新問題**: 52**
あなたの会社では、オンプレミスの QRadar を SIEM ソリューションとして使用しています。これをクラウドの Rapid7 に置き換えようとしています。従来のオンプレミスの QRadar は、最終的には廃止される予定です。IT 部門は、QRadar が使用するトークンと同じトークンを使用したくありません。
A. Netskope は複数の REST API トークンをサポートしていません。
B. イベントを共有するための複数のトークンをサポートするには、Netskope REST API v1 を使用する必要があります。
C. イベントを共有するための複数のトークンをサポートするには、Netskope REST API v2 を使用する必要があります。
D. 複数のトークンをサポートしてイベントを共有するには、Advanced Threat Protection ライセンスを使用する必要があります。
Answer: C (メーッセージを残す**)**
Netskope REST API v2 は複数のトークンをサポートしており、異なるアプリケーションや統合 (QRadar や Rapid7 など) が個別のトークンを持つことができます。これにより、トークンの競合を回避し、異なる SIEM システムのアクセス権限を分離することでセキュリティを強化します。

最新問題**: 53**
Skope IT を使用してセキュリティ インシデントを分析し、相関関係を調べています。API ポリシーによって生成されたイベントが多すぎます。Netskope クライアントによって生成されたログのみをフィルター処理したいと考えています。
A. access_method フィルターを使用して、ドロップダウン メニューからクライアントを選択します。
B. access_method フィルターを使用して、ドロップダウン メニューから [トンネル] を選択します。
C. access_method フィルターを使用して、ドロップダウン メニューから [ログ] を選択します。
D. クエリ モードを使用し、access_method neq Client を使用します。
Answer: A (メーッセージを残す**)**
Netskope クライアントによって生成されたログをフィルタリングするには、Skope IT の access_method フィルタ ドロップダウン メニューから [クライアント] を選択します。このフィルタを使用すると、管理者はアクセス方法別にログを絞り込むことができるため、Netskope クライアントにのみ関連する問題のトラブルシューティングが容易になります。

最新問題**: 54**

顧客は、すべてのアプリケーションを Microsoft 365 と Azure に移行しています。適切なプラクティスとポリシー (またはインライン トラフィック) が導入されていますが、再構成を継続的に検出し、コンプライアンス標準を適用したいと考えています。
どの 2 つのソリューションが要件を満たすでしょうか? (2 つ選択してください。)
A. Netskope SaaS セキュリティ態勢管理
B. Netskope クラウド信頼度指数
C. Netskope リスクインサイト
D. Netskope 継続的セキュリティ評価
Answer: A,D (メーッセージを残す)
Microsoft 365 および Azure アプリケーションのコンプライアンス標準を継続的に検出して適用するには、Netskope SaaS Security Posture Management (SSPM) と Netskope Continuous Security Assessment (CSA) を使用する必要があります。Netskope SSPM を使用すると、Microsoft 365 などの SaaS 環境におけるセキュリティ、アクセス許可、アクセス関連の問題を監視、評価し、対処することができます。Netskope SSPM は、SaaS アプリの設定をセキュリティ ポリシーや業界ベンチマーク (CIS、PCI-DSS、NIST、HIPAA、CSA、GDPR、AIPCA、ISO など) と比較することで、セキュリティ ポスチャを継続的にチェックします。また、管理対象アプリに接続されているサードパーティ アプリの可視性と制御も提供します1。Netskope CSA を使用すると、Azure などの IaaS 環境における構成ミスを検出し、監査し、修正することができます。
Netskope CSA は、業界標準、CIS ベンチマーク、規制フレームワークに照らしてクラウド構成を継続的に監視および監査します。また、パブリック クラウドを脅威やデータ損失から保護するためのリアルタイムのインライン保護も提供します2。したがって、オプション A と D は正しく、その他のオプションは誤りです。参考資料: SaaS セキュリティ ポスチャ管理 - Netskope、パブリック クラウド セキュリティ ソリューション - Netskope

最新問題: 55
あなたのチームは、10 件の Netskope DLP インシデントを調査するように依頼されています。これらのインシデントをさまざまなチーム メンバーに割り当てる必要があります。
A. チケットツールを使用します。
B. フォレンジックインシデントワークフローを使用します。
C. DLP インシデント ワークフローを使用します。
D. 隔離インシデント ワークフローを使用します。
Answer: C (メーッセージを残す)
Netskope の DLP インシデント ワークフローは、DLP インシデントの管理と調査のために特別に設計されています。このワークフローにより、インシデントをチーム メンバーに割り当てることができるため、データ損失の懸念事項の効率的な調査と解決が容易になります。