

Cisco Web セキュリティ アプライアンス 10 v1.1

最終更新日: 2018 年 2 月 16 日

このデモンストレーションについて

この事前設定済みデモンストレーションのガイドには、次の内容が含まれています。

[要件](#)

[このソリューションについて](#)

[トポロジ](#)

[はじめに](#)

[シナリオ 1: Web セキュリティ アプライアンス ダッシュボードの概要](#)

[シナリオ 2: アクセス ポリシー](#)

[シナリオ 3: 識別プロファイル](#)

[シナリオ 4: レポート](#)

要件

次の表に、本デモンストレーションに必要な要件の概要を示します。

表 1. 要件

必須	オプション
<ul style="list-style-type: none">• Cisco AnyConnect® がインストールされているラップトップ	<ul style="list-style-type: none">• オプションの要件はありません

このソリューションについて

Cisco Web セキュリティ アプライアンスは、インターネットトラフィックを傍受および監視するとともに、ポリシーを適用することによって、マルウェア、機密データ損失、生産性低下、その他のインターネット ベースの脅威から社内ネットワークを保護することに役立ちます。1 つのソリューションで、高度な脅威防御、高度なマルウェア防御 (AMP)、アプリケーションの可視性と制御 (AVC)、洞察力に富んだレポート、セキュアモビリティなどの機能を兼ね備えています。また、Web トラフィックの保護とコントロールを行いながら、導入を単純化し、コストを削減します。

新しい AsyncOS 10 リリースでは、リファラー ヘッダー バイパスのサポート、外部フィード処理、中間証明書サポートのほか、ユーザ エージェント リストの更新、AMP プライベート クラウド サポート、AMP レポートの強化の新機能が追加されています。

トポロジ

このコンテンツには、スクリプト形式のシナリオと、ソリューションの機能を実例で示すために事前設定されたユーザとコンポーネントが含まれています。コンポーネントのほとんどは、管理ユーザ アカウントを使用して任意の設定が可能です。コンポーネントへのアクセスに使用する IP アドレスとユーザ アカウント資格情報は、アクティブ セッションの [トポロジ (Topology)] メニューのコンポーネント アイコンをクリックして確認するか、それらを必要とするシナリオ内の手順で確認できます。

図 1. dCloud のトポロジ

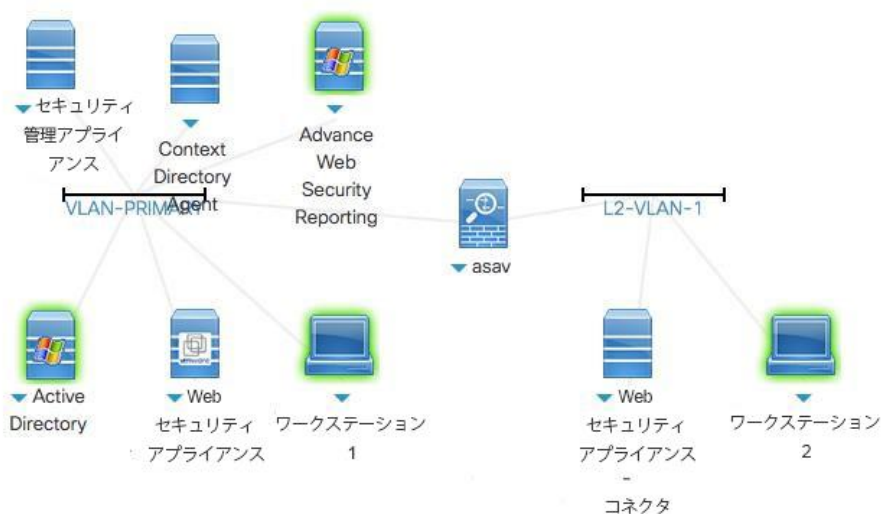


表 2. 機器の詳細

名前	説明	ホスト名 (FQDN)	IP アドレス	ユーザ名	パスワード
WSA-HQ1 プロキシ	WSA-HQ1 プロキシ		198.18.133.51:8080	admin	C1sco12345
WSA-HQ2 プロキシ	WSA-HQ2 プロキシ		198.18.133.52:8080	admin	C1sco12345
WSA コネクタ	WSA コネクタ		198.19.10.53:8080	admin	C1sco12345
SMA	セキュリティ管理アプライアンス		198.18.133.55	admin	C1sco12345

はじめに

プレゼンテーションの前に

Cisco dCloud では、実際の対象者の前でプレゼンテーションを行う前に、アクティブなセッションを使用して、このドキュメントのタスクを実施しておくことを強く推奨します。そうすることで、ドキュメントとコンテンツの構成に慣れることができます。

場合によっては、環境を元の構成にリセットするため、このガイドに従った後に新しいセッションをスケジュールする必要があります。

プレゼンテーションを成功させるためには、入念な準備が不可欠です。

次の手順に従ってコンテンツのセッションをスケジュールし、プレゼンテーション環境を設定します。

1. dCloud セッションを開始します。[\[手順を見る\]](#)

注:セッションがアクティブになるまで最長で 10 分かかることがあります。

2. 最適なパフォーマンスを得るために、Cisco AnyConnect VPN [\[手順を見る\]](#) およびラップトップのローカル RDP クライアント[\[手順を見る\]](#) を使用してワークステーションに接続します。

ワークステーション 1: 198.18.133.36、ユーザ名: dcloud\wsaproxy、パスワード: C1sco12345

注: Cisco dCloud リモート デスクトップ クライアントを使用してワークステーションに接続することもできます [\[手順を見る\]](#)。dCloud リモート デスクトップ クライアントは、最小限の操作でアクティブ セッションにアクセスする場合に最適です。ただし、この方法には、接続ができない場合や、パフォーマンスが悪い場合があります。

シナリオ 1: Web セキュリティ アプライアンス ダッシュボードの概要

手順


1. ダッシュボードの上部には、システム アクティビティが表示されます。

[システムの概要(System Overview)]: Web プロキシのトラフィックに関する情報が含まれます

[システムリソース使用率(System Resource Utilization)]: CPU 使用率、RAM 使用量、ディスク使用率に関する情報

My Dashboard

 Printable PDF 

Attention —  You can customize this "My Dashboard" page by adding report modules from different reports. Some modules are added for you by default. The Overview page can be accessed from [Reporting > Overview](#).



2. ダッシュボードの下部には、Web アクティビティが表示されます。

[Web プロキシアクティビティ総数(Total Web Proxy Activity)]

[疑わしいトランザクション(Suspected Transactions)] と [正常なトランザクション(Clean Transactions)] に関する Web プロキシの概要

[疑わしいトランザクション(Suspected Transactions)]

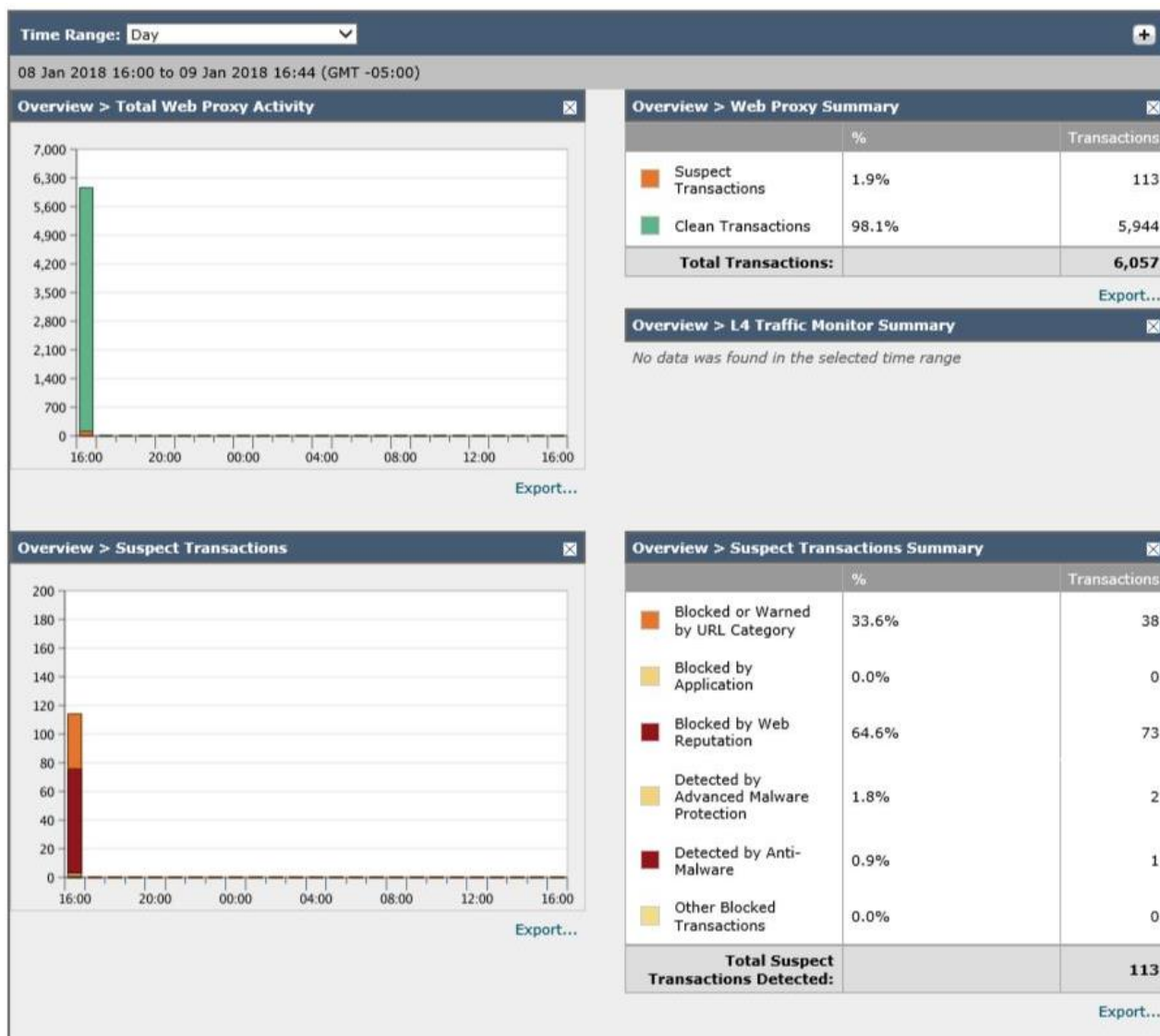
[疑わしいトランザクションの概要(Suspect Transactions Summary)]

[URL カテゴリごとの上位トランザクション(Top Transactions by URL category)]

[アプリケーションの種類ごとの上位トランザクション(Top Transactions by Application Type)]

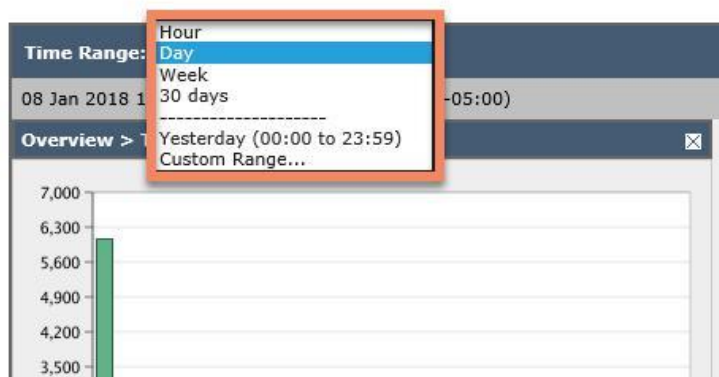
監視およびブロックされた [上位のマルウェアカテゴリ(Top Malware Categories)]

ブロックまたは警告された [上位ユーザ(Top Users)]





3. 上にスクロールし、時間範囲を調整します(選択に応じて、データがどのように更新されるかを確認します)

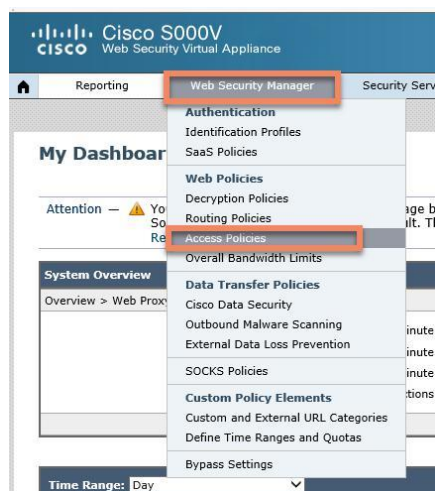


シナリオ 2: アクセス ポリシー

手順

アクセス ポリシー機能は、管理者が URL とブロックするマルウェアを設定するために使用します。

1. ダッシュボードから、[Web セキュリティ マネージャ (Web Security Manager)] > [アクセスポリシー (Access Policies)] の順に選択します。



2. デモには、事前に定義されたアクセス ポリシーが含まれています。[AP マーケティング (AP Marketing)] をクリックします。

Access Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
1	AP CEO Identification Profile: All All identified users	(global policy)	Block: 12 Warn: 5 Monitor: 71 Safe Search: Block All Unsafe Search Site Content Rating: Block	(global policy)	(global policy)	(global policy)	
2	AP Finance Identification Profile: All 1 groups (...)	(global policy)	Block: 11 Warn: 5 Monitor: 71 Quota-Based: 1 Safe Search: Block All Unsafe Search Site Content Rating: Block	Block: 1 Restrict: 1 Monitor: 362	(global policy)	(global policy)	
3	AP Marketing Identification Profile: All 1 groups (...)	(global policy)	Block: 11 Warn: 5 Monitor: 69 Quota-Based: 1 Safe Search: Block All Unsafe Search Site Content Rating: Block	(global policy)	(global policy)	(global policy)	
	Global Policy Identification Profile: All	No blocked items	Block: 11 Warn: 5 Monitor: 70 Safe Search: Block All Unsafe Search Site Content Rating: Block	Monitor: 364	No blocked items	Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled	

3. [アクセスポリシー(Access Policy)] ページには、ポリシー設定とメンバー定義が表示されます。

Access Policy: AP Marketing

Policy Settings

Enable Policy

Policy Name: ?

AP Marketing
(e.g. my IT policy)

Description:

Insert Above Policy: 3 (Global Policy) ▼

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

All Identification Profiles ▼

All Authenticated Users
 Selected Groups and Users ?

Groups:
Realm: dCloud.cisco.com
 DCLLOUD\Marketing
 Users: No users entered

Guests (users failing authentication)
 All Users (authenticated and unauthenticated users)

If the "All Users" option is selected, at least one Advanced membership option must also be selected.

▶ Advanced
Define additional group membership criteria.

Cancel
Submit

4. **グループ リンク**をクリックします。グループが Active Directory から取得されます。[グループの編集(Edit Groups)] ページでは、アクセス ポリシーからグループを追加または削除できます。
5. グループのいずれかを選択して、[追加(Add)] をクリックします。グループがポリシーに追加されます。

Access Policies: Policy "AP Marketing": Edit Groups

Authorized Groups

Start typing a group name into the Directory Search field to see matching entries from the directory. For Active Directory groups, omit the domain name (for instance, type "group" to find "DOMAIN\Group1"). The search is case-insensitive. The wildcard character "*" may be used. However, it cannot be used as the last character.

Select items from the Directory Search list and press Add to add them to the Authorized Groups list. Alternatively, you can type the entire name (for instance, to add a group that belongs to a trusted domain or a group that is not yet available in the directory). If group(s) are added that already exist in the Authorized Group list, the duplicates will be automatically omitted.

Note: It is not recommended to add more than 300 groups in an access policy because it may result in authentication failures.

Realm: dCloud.cisco.com

Directory Search: ?

Directory search completed (88 matches).

Realm: dCloud.cisco.com
 DCLLOUD\K31000-8MSE775V7HFV
 DCLLOUD\Account Operators
 DCLLOUD\Administrators
 DCLLOUD\Allowed RODC Password Replication Gro
 DCLLOUD\Backup Operators
 DCLLOUD\Cert Publishers
 DCLLOUD\Certificate Service DCOM Access
 DCLLOUD\CISCO_ICM_CONFIG
 DCLLOUD\CISCO_ICM_SETUP
 DCLLOUD\CISCO_ICM_WEBVIEW
 DCLLOUD\Cryptographic Operators
 DCLLOUD\Delegated Setup
 DCLLOUD\Denied RODC Password Replication Gro
 DCLLOUD\DEVICE-ADMINS
 DCLLOUD\DHCP Administrators
 DCLLOUD\DHCP Users
 DCLLOUD\Discovery Management
 DCLLOUD\Distributed COM Users
 DCLLOUD\DnsAdmins

Add =>

Selected Groups

Realm: dCloud.cisco.com
 DCLLOUD\Marketing

Remove

Cancel
Done

6. [Web セキュリティマネージャ (Web Security Manager)] > [アクセスポリシー (Access Policies)] の順に選択して、アクセス ポリシーに戻ります。
7. [AP マーケティング (AP Marketing)] の [URL フィルタリング (URL filtering)] カテゴリをクリックします。監視されているカテゴリとブロックされているカテゴリが確認できます。

Access Policies

Policies							
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
1	AP CEO Identification Profile: All All identified users	(global policy)	Block: 12 Warn: 5 Monitor: 71 Safe Search: Block All Unsafe Search Site Content Rating: Block	(global policy)	(global policy)	(global policy)	
2	AP Finance Identification Profile: All 1 groups (...)	(global policy)	Block: 11 Warn: 5 Monitor: 71 Quota-Based: 1 Safe Search: Block All Unsafe Search Site Content Rating: Block	Block: 1 Restrict: 1 Monitor: 362	(global policy)	(global policy)	
3	AP Marketing Identification Profile: All 1 groups (...)	(global policy)	Block: 11 Warn: 5 Monitor: 69 Quota-Based: 1 Safe Search: Block All Unsafe Search Site Content Rating: Block	(global policy)	(global policy)	(global policy)	
	Global Policy Identification Profile: All	No blocked items	Block: 11 Warn: 5 Monitor: 70 Safe Search: Block All Unsafe Search Site Content Rating: Block	Monitor: 364	No blocked items	Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled	

8. この画面では、事前に定義された URL カテゴリが表示されます。お客様は、この定義済みカテゴリを使用して、自身のアクセプタブルユース ポリシーを定義することができます。

Access Policies: URL Filtering: AP Marketing

Custom and External URL Category Filtering								
<small>These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.</small>								
Category	Category Type	Use Global Settings	Override Global Settings					Quota
			Block	Redirect	Allow	Monitor	Warn	
Cisco Software	Custom (Local)	<input checked="" type="checkbox"/>	Select all	Select all	Select all	Select all	Select all	

Predefined URL Category Filtering							
<small>These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.</small>							
Category	Use Global Settings	Block	Monitor	Warn	Quota		
						Select all	Select all
Adult	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Advertisements	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Alcohol	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Arts	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Astrology	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Auctions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Business and Industry	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Chat and Instant Messaging	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Cheating and Plagiarism	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Child Abuse Content	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Computer Security	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Computers and Internet	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
DIY Projects	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Dating	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Digital Postcards	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Dining and Drinking	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Dynamic and Residential	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Education	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
Entertainment	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

9. [ストリーミング オーディオ (streaming audio)] カテゴリまでスクロール ダウンします。これはクォータ プロファイルで、ユーザがそのカテゴリを使用できる時間の上限(帯域幅での指定も可能)を設定できます。

Category	Select all	Block ⓧ	Monitor ⓧ	Warn ? ⓧ	Quota-Based ⓧ	Time-Based (Unavailable)
Pornography	✓					
Professional Networking	✓					
Real Estate	✓					
Reference	✓					
Religion	✓					
SaaS and B2B	✓					
Safe for Kids	✓					
Science and Technology	✓					
Search Engines and Portals	✓					
Sex Education	✓					
Shopping	✓					
Social Networking	✓					
Social Science	✓					
Society and Culture	✓					
Software Updates	✓					
Sports and Recreation	✓					
Streaming Audio Predefined Quota Profile: Limit Media	✓				✓	
Streaming Video	✓					
Tobacco	✓					
Transportation	✓					

10. メニューから、[Web セキュリティマネージャ (Web Security Manager)] > [時間範囲およびクォータの定義 (Define Time Ranges and Quotas)] の順に選択します。

11. [メディア制限 (Limit Media)] をクリックします。事前にクォータが定められています。時間とボリュームのクォータを確認します。クォータのリセット時間を定めることもできます。

Reporting	Web Security Manager	Security Services	Network	System Administration
Time Ranges and Quotas				
Time Ranges				
Add Time Range...				
No time ranges have been defined. Define time ranges for use in time-based policies.				
Daily Time and Volume Quotas				
Add Quota...				
Quota Name	Reset Time / Time Range	Time Quota	Volume Quota	Delete
Limit Media	12:00 AM ApplianceTimezone	4 Hrs 0 Min	3 GB	🗑️

12. メニューから、[Web セキュリティマネージャ (Web Security Manager)] > [カスタムおよび外部 URL (Custom and External URL)] カテゴリの順に選択します。

Custom and External URL Categories

Categories List					
Add Category...					
Order	Category	Category Type	Last Updated	Feed Content	Delete
1	Cisco Software	Custom (Local)	N/A	-	🗑️
2	Cisco	Custom (Local)	N/A	-	🗑️
3	Global Access Block List	Custom (Local)	N/A	-	🗑️
4	Global Access Allow List	Custom (Local)	N/A	-	🗑️
5	O365 Feed PassThru	External Feed	09 Jan 2018 16:35:15 PM	View	🗑️

13. [シスコ ソフトウェア (Cisco Software)] をクリックします。このカテゴリは、software.cisco.com にリダイレクトするように設定されています。この画面では、IP アドレス、ドメイン、URL、正規表現も定義できるため、ブロッキングや監視の対象を詳細に設定することができます。

Custom and External URL Categories: Edit Category

Edit Custom and External URL Category	
Category Name:	<input type="text" value="Cisco"/>
List Order:	<input type="text" value="2"/>
Category Type:	Local Custom Category
Sites: (?)	<div style="border: 1px solid gray; height: 100px; width: 100%;"></div> <p style="font-size: small;">(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)</p>
Sort URLs	<p style="font-size: x-small;">Click the Sort URLs button to sort all site URLs in Alpha-numerical order.</p>
Advanced	Regular Expressions: (?) <input type="text" value=".cisco.com"/> <p style="font-size: x-small;">Enter one regular expression per line.</p>

Cancel

Submit

14. [Web セキュリティマネージャ (Web Security Manager)] > [アクセスポリシー (Access Policies)] の順に選択して、アクセス ポリシーに戻ります。
15. [AP マーケティング (AP Marketing)] の [URL フィルタリング (URL filtering)] カテゴリをクリックし、[埋め込みおよび参照コンテンツのブロックの例外 (Exceptions to Blocking for Embedded/Referred Content)] までスクロール ダウンします。これにより、特定のコンテンツが特定のソースからアクセスされるのを制限することができます。
16. 例では、シスコのソフトウェアにはシスコドメイン上のユーザしかアクセスできないようになっています。

Exceptions to Blocking for Embedded/Referred Content		
<p style="font-size: x-small;">A web site may embed or refer to content that is categorized as a different category, or that is considered an application. For example, a News web site could contain content categorized as Streaming Video, and that is identified as being the application Youtube. By default, embedded content is blocked or monitored based on the action selected for its own category / application, regardless of what web site it is embedded in. Use this table to set exceptions (e.g., to permit all content referred from News web sites, or from a custom category representing your intranet).</p>		
<input checked="" type="checkbox"/> Enable Referrer Exceptions		
Set Exception for Content Referred by These Categories:	Set Exception for This Referred Content:	Add Exception
Cisco	selected embedded / referred content	<div style="border: 2px solid orange; padding: 2px;"> Categories: Cisco Software Applications: Click to select applications... </div>

Cancel

Submit

17. [Web セキュリティマネージャ (Web Security Manager)] > [アクセスポリシー (Access Policies)] の順に選択して、アクセス ポリシーに戻ります。

18. [AP ファイナンス (AP Finance)] の [アプリケーション (Applications)] をクリックします。

Access Policies

Policies							
Add Policy...							
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	Delete
1	AP CEO Identification Profile: All All identified users	(global policy)	Block: 12 Warn: 5 Monitor: 71 Safe Search: Block All Unsafe Search Site Content Rating: Block	(global policy)	(global policy)	(global policy)	
2	AP Finance Identification Profile: All 1 groups (...)	(global policy)	Block: 11 Warn: 5 Monitor: 71 Quota-Based: 1 Safe Search: Block All Unsafe Search Site Content Rating: Block	Block: 1 Restrict: 1 Monitor: 362	(global policy)	(global policy)	
3	AP Marketing Identification Profile: All 1 groups (...)	(global policy)	Block: 11 Warn: 5 Monitor: 69 Quota-Based: 1 Safe Search: Block All Unsafe Search Site Content Rating: Block	(global policy)	(global policy)	(global policy)	
	Global Policy Identification Profile: All	No blocked items	Block: 11 Warn: 5 Monitor: 70 Safe Search: Block All Unsafe Search Site Content Rating: Block	Monitor: 364	No blocked items	Web Reputation: Enabled Advanced Malware Protection: Enabled Anti-Malware Scanning: Enabled	
Edit Policy Order...							

19. [アプリケーションの可視性と制御 (Application Visibility and Control)] 画面が表示されます。この画面では、特定の Web アプリケーションを検索し、パラメーターまたは制限を設定することができます。

20. スクロール ダウンして、[インスタントメッセージ (Instant Messaging)] カテゴリに設定されている制限を確認します。プラス記号をクリックすると、制限の詳細を開くことができます。たとえば、このデモでは、Yahoo Messenger がブロックされています。

Applications Settings

Browse Application Types ▾

To identify some applications, inspection of HTTPS content may be required. For best efficacy, enable the HTTPS Proxy, then enables decryption for application visibility and control (see Security Services > HTTPS Proxy).

Applications	Settings
Edit all...	
Instant Messaging	
AirAIM	Use Global (Monitor)
AOL Instant Messenger	Use Global (Monitor)
Baiduhi	Use Global (Monitor)
CGIIRC	Use Global (Monitor)
Chatroulette	Use Global (Monitor)
Google Talk	Use Global (Monitor)
Icq2go	Use Global (Monitor)
ILoveIM	Use Global (Monitor)
KoolIM	Use Global (Monitor)
Mail.Ru Agent	Use Global (Monitor)
MessengerFX	Use Global (Monitor)
Mibbit	Use Global (Monitor)
Sinawebuc	Use Global (Monitor)
Webfetion	Use Global (Monitor)
WebQQ	Use Global (Monitor)
Webwangwang	Use Global (Monitor)
Wechat_web	Use Global (Monitor)
Windows Live Messenger	Use Global (Monitor)
Yahoo Messenger	Block
Edit all	

21. [アプリケーションを検索 (Search for Applications)] ドロップ ダウンをクリックします。「gmail」と入力すると、gmail の添付ファイルのダウンロードが制限されているのが確認できます。

Access Policies: Applications Visibility and Control: AP Finance

Edit Applications Settings

Define Applications Custom Settings ▾

Applications Settings

Search for Applications ▾ Applications Info ⓘ

Filter By:

Application Type: All ▾

Application Name: Starts With ▾ gmail

Current Action: All ▾

Application Types	Applications ▲	Actions
Webmail	Gmail	Restrict: Block File Attachment Download

Total: 364 Applications (1 Blocked, 1 Restricted, 362 Monitored)
Current Search: 1 Application (1 Restricted)

Cancel Submit

22. [制限(Restrict)]リンクをクリックして、ブロックの詳細を確認します。

Access Policies: Applications Visibility and Control: AP Finance

Edit Applications Settings

Define Applications Custom Settings ▾

Applications Settings

Search for Applications ▾ Applications Info ⓘ

Filter By:
Application Type: All ▾
Application Name: Starts With ▾
Current Action: All ▾

Application Types	Applications ▲	Actions
Webmail	Gmail	<div style="border: 2px solid orange; padding: 5px;">Set action for application Gmail <input type="radio"/> Use Global Setting (Monitor) <input checked="" type="radio"/> Monitor <input type="checkbox"/> Block File Attachment Upload <input checked="" type="checkbox"/> Block File Attachment Download <input type="checkbox"/> Block Sending Email <input type="radio"/> Block</div>

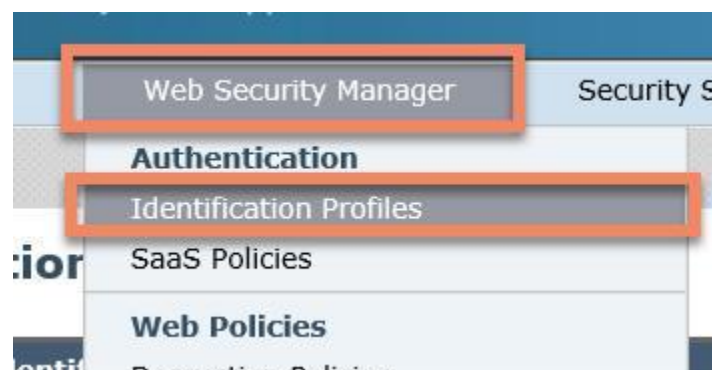
Total: 364 Applications (1 Blocked, 1 Restricted, 362 Monitored)
Current Search: 1 Application (1 Restricted)

シナリオ 3: 識別プロファイル

手順

識別ポリシーは、複数のサブネットまたはプロトコルを特定のポリシーに組み込む手段として、アクセス ポリシーや復号ポリシーに関連付けられています。

1. ダッシュボードから、[Web セキュリティマネージャ (Web Security Manager)] > [識別ポリシー (Identification Policies)] の順に選択します。



2. デモには、事前に定義されたアクセス プロファイルが含まれています。[認証バイパス (Auth Bypass)] に、認証を除外されるサブネットが含まれていることを確認します。

Identification Profiles

Client / User Identification Profiles				
Add Identification Profile...				
Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
1	Auth Bypass Subnets: 10.1.1.1, 10.1.1.2, 198.18.133.222, 10.16.3.143 Protocols: HTTP/HTTPS	Exempt from Authentication / User Identification	(global profile)	
2	Apple Devices Protocols: HTTP/HTTPS User Agent: Safari: Safari Any Versions	Authenticate: Realm: dCloud.cisco.com (Scheme: Kerberos)	(global profile)	
3	Global Authentication Policy Protocols: HTTP/HTTPS	Authenticate: Realm: dCloud.cisco.com (Scheme: Basic, NTLMSSP)	(global profile)	
Global Identification Profile		Authenticate: Realm: dCloud.cisco.com (Scheme: Basic, NTLMSSP, Kerberos) Guest privileges for users failing authentication	Exempt	

Edit Order...

3. [Apple デバイス (Apple Devices)] プロファイルの [プロトコル (Protocols)] には [HTTP/HTTPS] が指定され、[ユーザ エージェント (User Agent)] には、Safari のバージョンが指定されています。Kerberos 認証が必要となるように、ポリシーが設定されています。

Identification Profiles

Client / User Identification Profiles				
Add Identification Profile...				
Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
1	Auth Bypass Subnets: 10.1.1.1, 10.1.1.2, 198.18.133.222, 10.16.3.143 Protocols: HTTP/HTTPS	Exempt from Authentication / User Identification	(global profile)	
2	Apple Devices Protocols: HTTP/HTTPS User Agent: Safari: Safari Any Versions	Authenticate: Realm: dCloud.cisco.com (Scheme: Kerberos)	(global profile)	
3	Global Authentication Policy Protocols: HTTP/HTTPS	Authenticate: Realm: dCloud.cisco.com (Scheme: Basic, NTLMSSP)	(global profile)	
Global Identification Profile		Authenticate: Realm: dCloud.cisco.com (Scheme: Basic, NTLMSSP, Kerberos) Guest privileges for users failing authentication	Exempt	

Edit Order...

4. [グローバル認証ポリシー (Global Authentication Policy)] では、その他のすべてがカバーされています。

Identification Profiles

Client / User Identification Profiles				
Add Identification Profile...				
Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
1	Auth Bypass Subnets: 10.1.1.1, 10.1.1.2, 198.18.133.222, 10.16.3.143 Protocols: HTTP/HTTPS	Exempt from Authentication / User Identification	(global profile)	
2	Apple Devices Protocols: HTTP/HTTPS User Agent: Safari: Safari Any Versions	Authenticate: Realm: dCloud.cisco.com (Scheme: Kerberos)	(global profile)	
3	Global Authentication Policy Protocols: HTTP/HTTPS	Authenticate: Realm: dCloud.cisco.com (Scheme: Basic, NTLMSSP)	(global profile)	
Global Identification Profile		Authenticate: Realm: dCloud.cisco.com (Scheme: Basic, NTLMSSP, Kerberos) Guest privileges for users failing authentication	Exempt	

Edit Order...

- ダッシュボードから、[Web セキュリティ マネージャ (Web Security Manager)] > [復号ポリシー (Decryption Policies)] の順に選択します。
- 復号ポリシーは、SSL 復号を適用している管理者に適用されます。[DP ユーザグループ (DP User Groups)] をクリックします。

Decryption Policies

Policies						
Order	Group	URL Filtering	Web Reputation	Default Action	Delete	
1	DP User Groups Identification Profile: All 3 groups (...)	Pass Through: 2 Monitor: 2 Decrypt: 82 Drop: 1	(global policy)	(global policy)		
2	DP CEO Identification Profile: All All identified users	Pass Through: 2 Monitor: 2 Decrypt: 82 Drop: 1	(global policy)	(global policy)		
3	DP Passthru Identification Profile: All All identified users URL Categories: Global Access Allow List, Cisco Software, Cisco,...	Pass Through: 3 Monitor: 1	(global policy)	Pass Through		
	Global Policy Identification Profile: All	Pass Through: 2 Decrypt: 82 Drop: 1	Enabled	Decrypt		

- [DP ユーザグループ (DP User Groups)] ページには、ポリシーが適用される**グループ**が表示されます。

Decryption Policy: DP User Groups

Policy Settings	
<input checked="" type="checkbox"/> Enable Policy	
Policy Name: ?	DP User Groups <small>(e.g. my IT policy)</small>
Description:	<input type="text"/>
Insert Above Policy:	1 (DP CEO) ▼

Policy Member Definition	
<i>Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.</i>	
Identification Profiles and Users:	<div style="border: 1px solid gray; padding: 5px;"> All Identification Profiles ▼ <input type="radio"/> All Authenticated Users <input checked="" type="radio"/> Selected Groups and Users ? Groups: Realm: dCloud.cisco.com DCLLOUD\Finance Users DCLLOUD\HR DCLLOUD\Marketing Users: No users entered <input type="radio"/> Guests (users failing authentication) <input type="radio"/> All Users (authenticated and unauthenticated users) </div>
<small>If the "All Users" option is selected, at least one Advanced membership option must also be selected. Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.</small>	
▶ Advanced	Define additional group membership criteria.

Cancel

Submit

8. [キャンセル(Cancel)] をクリックして、[復号ポリシー(Decryption Policies)] に戻り、[DP ユーザグループ(DP User Groups)] の [URL フィルタリング(URL Filtering)] をクリックします。

Decryption Policies

Policies					
Order	Group	URL Filtering	Web Reputation	Default Action	Delete
1	DP User Groups Identification Profile: All 3 groups (...)	Pass Through: 2 Monitor: 2 Decrypt: 82 Drop: 1	(global policy)	(global policy)	
2	DP CEO Identification Profile: All All identified users	Pass Through: 2 Monitor: 2 Decrypt: 82 Drop: 1	(global policy)	(global policy)	
3	DP Passthru Identification Profile: All All identified users URL Categories: Global Access Allow List, Cisco Software, Cisco,...	Pass Through: 3 Monitor: 1	(global policy)	Pass Through	
	Global Policy Identification Profile: All	Pass Through: 2 Decrypt: 82 Drop: 1	Enabled	Decrypt	

9. [DP ユーザグループ(DP User Groups)] の [URL フィルタリング(URL Filtering)] には、復号されるさまざまな種類のトラフィックが表示されます。

Decryption Policies: URL Filtering: DP User Groups

Custom and External URL Category Filtering									
<i>These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.</i>									
Category	Category Type	Use Global Settings	Override Global Settings					Quota-Based	Time-Based
			Pass Through	Monitor	Decrypt	Drop	(Unavailable)		
Global Access Block List	Custom (Local)	—	Select all	Select all	Select all	Select all	Select all	—	
Global Access Allow List	Custom (Local)	—	Select all	Select all	Select all	Select all	Select all	—	

Cancel

Submit

Predefined URL Category Filtering								
<i>These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.</i>								
Category	Use Global Settings	Override Global Settings					Quota-Based	Time-Based
		Pass Through	Monitor	Decrypt	Drop	(Unavailable)		
File Transfer Services	<input checked="" type="checkbox"/>	Select all	Select all	Select all	Select all	Select all	—	
Filter Avoidance	<input checked="" type="checkbox"/>	Select all	Select all	Select all	Select all	Select all	—	
Finance	<input checked="" type="checkbox"/>	Select all	Select all	Select all	Select all	Select all	—	
Freeware and Shareware	<input checked="" type="checkbox"/>	Select all	Select all	Select all	Select all	Select all	—	
Gambling	<input checked="" type="checkbox"/>	Select all	Select all	Select all	Select all	Select all	—	
Games	<input checked="" type="checkbox"/>	Select all	Select all	Select all	Select all	Select all	—	
Government and Law	<input checked="" type="checkbox"/>	Select all	Select all	Select all	Select all	Select all	—	
Hacking	<input checked="" type="checkbox"/>	Select all	Select all	Select all	Select all	Select all	—	
Hate Speech	<input checked="" type="checkbox"/>	Select all	Select all	Select all	Select all	Select all	—	
Health and Nutrition	<input checked="" type="checkbox"/>	Select all	Select all	Select all	Select all	Select all	—	
Humor	<input checked="" type="checkbox"/>	Select all	Select all	Select all	Select all	Select all	—	
Hunting	<input checked="" type="checkbox"/>	Select all	Select all	Select all	Select all	Select all	—	
Illegal Activities	<input checked="" type="checkbox"/>	Select all	Select all	Select all	Select all	Select all	—	

10. [キャンセル(Cancel)]をクリックして、[復号ポリシー(Decryption Policies)]に戻り、[DP パススルー(DP Passthru)]をクリックします。

Decryption Policies

Policies					
Order	Group	URL Filtering	Web Reputation	Default Action	Delete
1	DP User Groups Identification Profile: All 3 groups (...)	Pass Through: 2 Monitor: 2 Decrypt: 82 Drop: 1	(global policy)	(global policy)	
2	DP CEO Identification Profile: All All identified users	Pass Through: 2 Monitor: 2 Decrypt: 82 Drop: 1	(global policy)	(global policy)	
3	DP Passthru Identification Profile: All All identified users URL Categories: Global Access Allow List, Cisco Software, Cisco,...	Pass Through: 3 Monitor: 1	(global policy)	Pass Through	
	Global Policy Identification Profile: All	Pass Through: 2 Decrypt: 82 Drop: 1	Enabled	Decrypt	

11. これは、復号したくないポリシーに適用されます。このポリシーは、承認済みのすべてのユーザに適用されるため、グローバルです。

Decryption Policy: DP Passthru

Policy Settings

Enable Policy

Policy Name:
(e.g. my IT policy)

Description:

Insert Above Policy:

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

All Authenticated Users

Selected Groups and Users ?

Groups: No groups entered

Users: No users entered

Guests (users failing authentication)

All Users (authenticated and unauthenticated users)

If the "All Users" option is selected, at least one Advanced membership option must also be selected. Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.

Advanced

Use the Advanced options to define or edit membership by proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Proxy Ports: None Selected

Subnets: None Selected

Time Range: No Time Range Definitions Available
(see Web Security Manager > Defined Time Ranges)

12. [キャンセル(Cancel)] をクリックして、[復号ポリシー(Decryption Policies)] に戻り、[DP パススルー(DP Passthru)] の [URL フィルタリング(URL Filtering)] をクリックします。

Decryption Policies

Policies					
Order	Group	URL Filtering	Web Reputation	Default Action	Delete
1	DP User Groups Identification Profile: All 3 groups (...)	Pass Through: 2 Monitor: 2 Decrypt: 82 Drop: 1	(global policy)	(global policy)	
2	DP CEO Identification Profile: All All identified users	Pass Through: 2 Monitor: 2 Decrypt: 82 Drop: 1	(global policy)	(global policy)	
3	DP Passthru Identification Profile: All All identified users URL Categories: Global Access Allow List, Cisco Software, Cisco,...	Pass Through: 3 Monitor: 1	(global policy)	Pass Through	
	Global Policy Identification Profile: All	Pass Through: 2 Decrypt: 82 Drop: 1	Enabled	Decrypt	

13. パススルー ポリシーが、すべての Cisco ソフトウェアと Office 365 に適用されていることを確認します。

Decryption Policies: URL Filtering: DP Passthru

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Use Global Settings	Override Global Settings					Quota-Based	Time-Based
			Pass Through	Monitor	Decrypt	Drop	Drop		
		Select all	Select all	Select all	Select all	Select all		(Unavailable)	
Cisco Software	Custom (Local)	—	✓					—	
Cisco	Custom (Local)	—		✓				—	
Global Access Allow List	Custom (Local)	—	✓					—	
O365 Feed PassThru	External Feed	—	✓					—	

Cancel Submit

Predefined URL Category Filtering

No Predefined URL Categories are selected for this policy group.

Overall Web Activities Quota

Specify a quota that applies to all web surfing activities. When quotas are applied to specific URL Categories above, transactions in those categories will be counted against both the category quota and the overall quota. Typically, the overall quota should be larger than any category quota.

Predefined Quota Profile: Select Time and Volume Quota ...

Cancel Submit

Uncategorized URLs

This category is unavailable.

Cancel Submit

14. ダッシュボードから、[Web セキュリティマネージャ (Web Security Manager)] > [カスタムおよび外部 URL (Custom and External URL)] カテゴリを選択します。
15. [O365 フィードパススルー (O365 Feed PassThru)] をクリックします。

Custom and External URL Categories

Categories List					
Add Category...					
Order	Category	Category Type	Last Updated	Feed Content	Delete
1	Cisco Software	Custom (Local)	N/A	-	
2	Cisco	Custom (Local)	N/A	-	
3	Global Access Block List	Custom (Local)	N/A	-	
4	Global Access Allow List	Custom (Local)	N/A	-	
5	O365 Feed PassThru	External Feed	09 Jan 2018 16:35:15 PM	View	

16. Office 365 でのサポート機能が表示されます。[フィードファイルの場所 (Feed File Location)] を確認します。WSA 外部リストがフィードされ、カスタム URL カテゴリとして使用されます。

Custom and External URL Categories: Edit Category

Edit Custom and External URL Category	
Category Name:	<input type="text" value="O365 Feed PassThru"/>
List Order:	<input type="text" value="5"/>
Category Type:	External Live Feed Category
Routing Table:	Management
Feed File Location: ?	<input type="radio"/> Cisco Feed Format ? <input checked="" type="radio"/> Office 365 Feed Format ? Office 365 Feed Location: <input type="text" value="https://support.content.office.net"/> <input type="button" value="Get File"/>
Auto Update the Feed:	<input checked="" type="radio"/> Do not auto update <input type="radio"/> Hourly <input type="text" value="1"/> Every <input type="text" value="01:00"/> (HH:MM)

17. [キャンセル(Cancel)] をクリックして、[カスタムおよび外部 URL (Custom and External URL)] カテゴリに戻ります。[O365 フィードパススルー (O365 Feed PassThru)] の [フィード コンテンツ (Feed Content)] にある [表示 (View)] をクリックします。

Custom and External URL Categories

Categories List					
Add Category...					
Order	Category	Category Type	Last Updated	Feed Content	Delete
1	Cisco Software	Custom (Local)	N/A	-	
2	Cisco	Custom (Local)	N/A	-	
3	Global Access Block List	Custom (Local)	N/A	-	
4	Global Access Allow List	Custom (Local)	N/A	-	
5	O365 Feed PassThru	External Feed	09 Jan 2018 16:35:15 PM	View	

18. [O365 フィードパススルー (O365 Feed PassThru)] カテゴリに関連付けられた外部カテゴリ コンテンツの一覧が表示されます。

The dialog box titled "External Category Content" displays a list of IP addresses and subnets under the heading "Sites:". The list includes:

- 104.214.144.62/32
- 157.56.151.0/25
- 40.71.88.196/32
- 13.76.140.48/32
- 104.44.255.0/25
- 40.114.192.209/32
- 40.78.62.210/32
- 13.75.159.17/32
- 204.79.197.215/32
- 40.117.96.104/32
- 52.172.12.123/32
- 52.175.154.183/32
- 23.99.125.4/32
- 13.80.125.22/32
- 23.103.136.0/21
- 70.37.151.128/25
- 40.78.146.128/32
- 104.215.194.17/32
- 207.46.100.0/24
- 104.45.225.7/32
- 51.140.62.120/32
- 13.107.9.158/31
- 111.221.104.43/32
- 213.199.180.128/26

An "OK" button is visible at the bottom left of the dialog box.

19. [OK] をクリックします。
20. [O365 フィードパススルー (O365 Feed PassThru)] をクリックして、ポリシーを編集します。

21. [シスコフィード形式 (Cisco Feed Format)] を選択します。HTTP または HTTPS プロトコルを使用して、ホワイト リストに登録された URL (またはブラック リストに登録された URL) のその他の外部フィードを参照できます。

Custom and External URL Categories: Edit Category

Edit Custom and External URL Category	
Category Name:	<input type="text" value="O365 Feed PassThru"/>
List Order:	<input type="text" value="5"/>
Category Type:	External Live Feed Category
Routing Table:	Management
Feed File Location: ?	<input checked="" type="radio"/> Cisco Feed Format ? <input type="radio"/> Office 365 Feed Format ?
	<input type="text" value="HTTPS"/> <input type="text" value="https://support.content.office.net"/>
	Advanced
	<input type="button" value="Get File"/>
	<div style="border: 1px solid #ccc; height: 100px;"></div>
Auto Update the Feed:	<input checked="" type="radio"/> Do not auto update
	<input type="radio"/> Hourly <input type="text" value="01:00"/> (HH:MM)

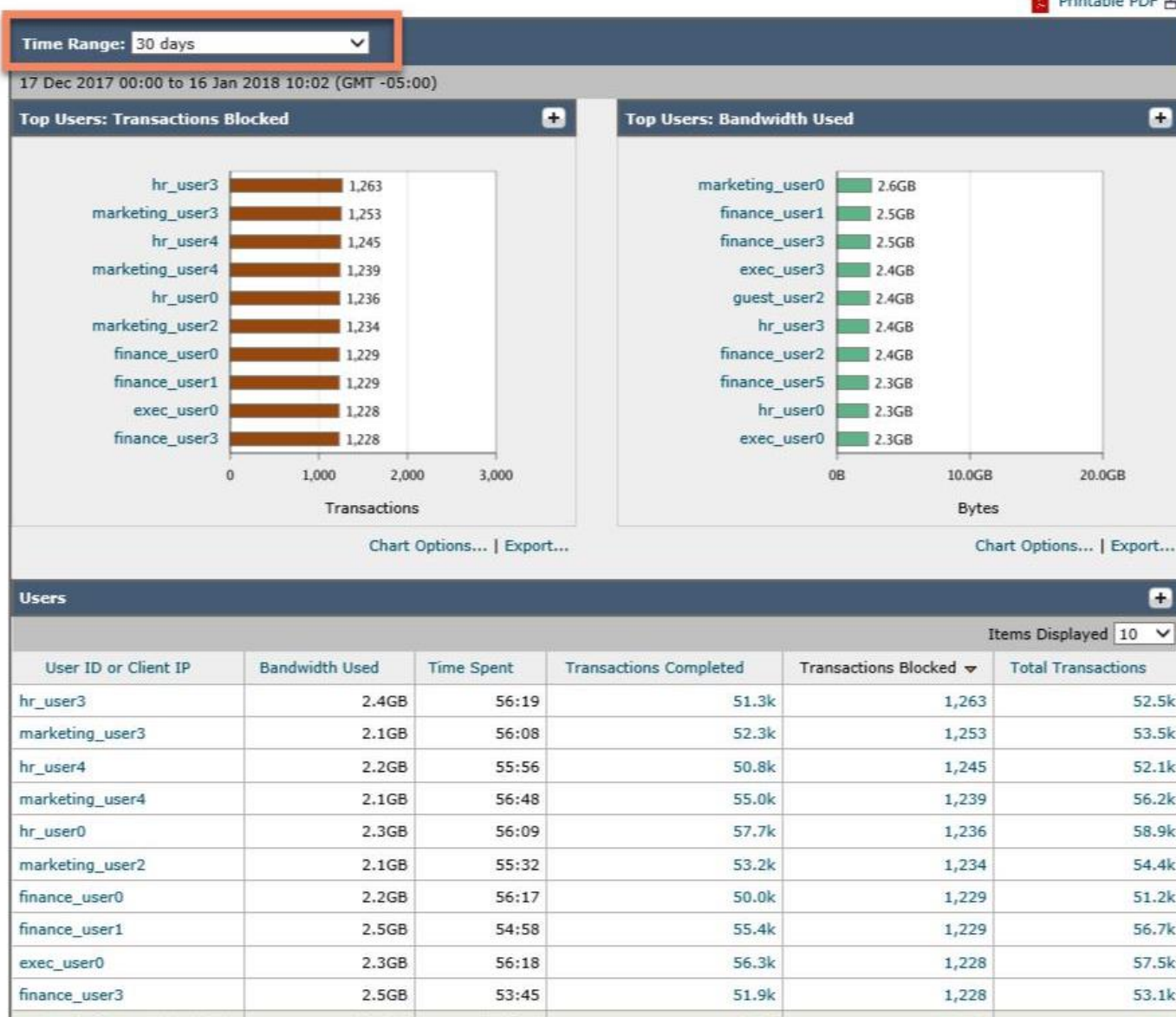
シナリオ 4: レポート

手順

1. メニューから [レポート(Reporting)] > [ユーザ(Users)] を選択します。このレポートには、トランザクション、使用帯域幅など、さまざまな特性に分類されたユーザの概要が表示されます。

注: データがすぐに表示されない場合は、時間範囲を 30 日に変更してください。

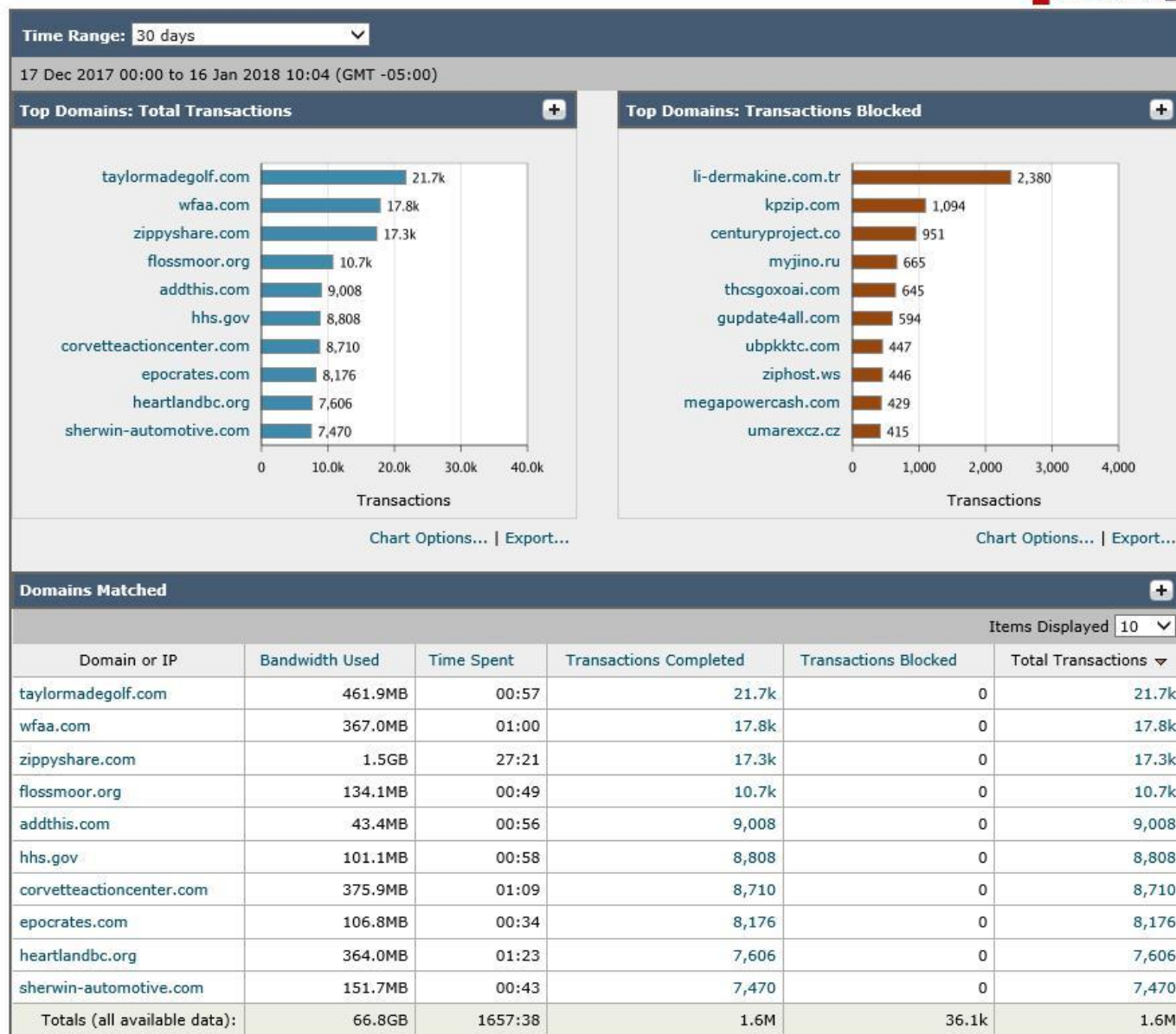
Users

Printable PDF 

2. メニューから [レポート(Reporting)] > [Web サイト(Web Sites)] を選択します。このレポートには、最上位ドメイン、ブロックされたトランザクション、一致するドメインにもとづいて Web サイトが表示されます。

Web Sites

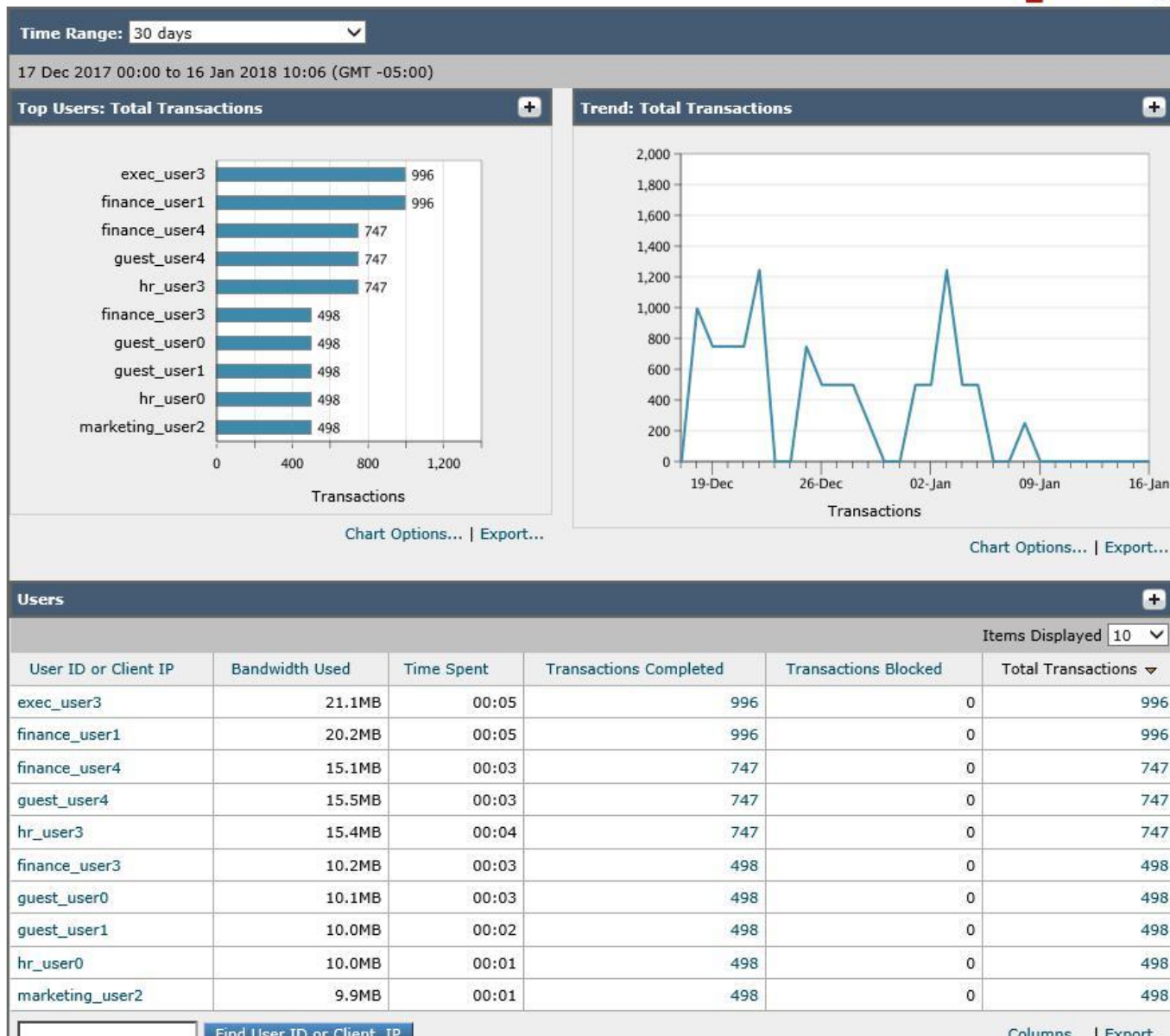
 Printable PDF



3. スクロール ダウンし、**Sherwin Automotive** というドメイン名をクリックします。上位ユーザ、総トランザクション、ユーザ、一致するカテゴリなどを含む Web サイトの詳細が表示されます。

Web Sites > sherwin-automotive.com

Printable PDF



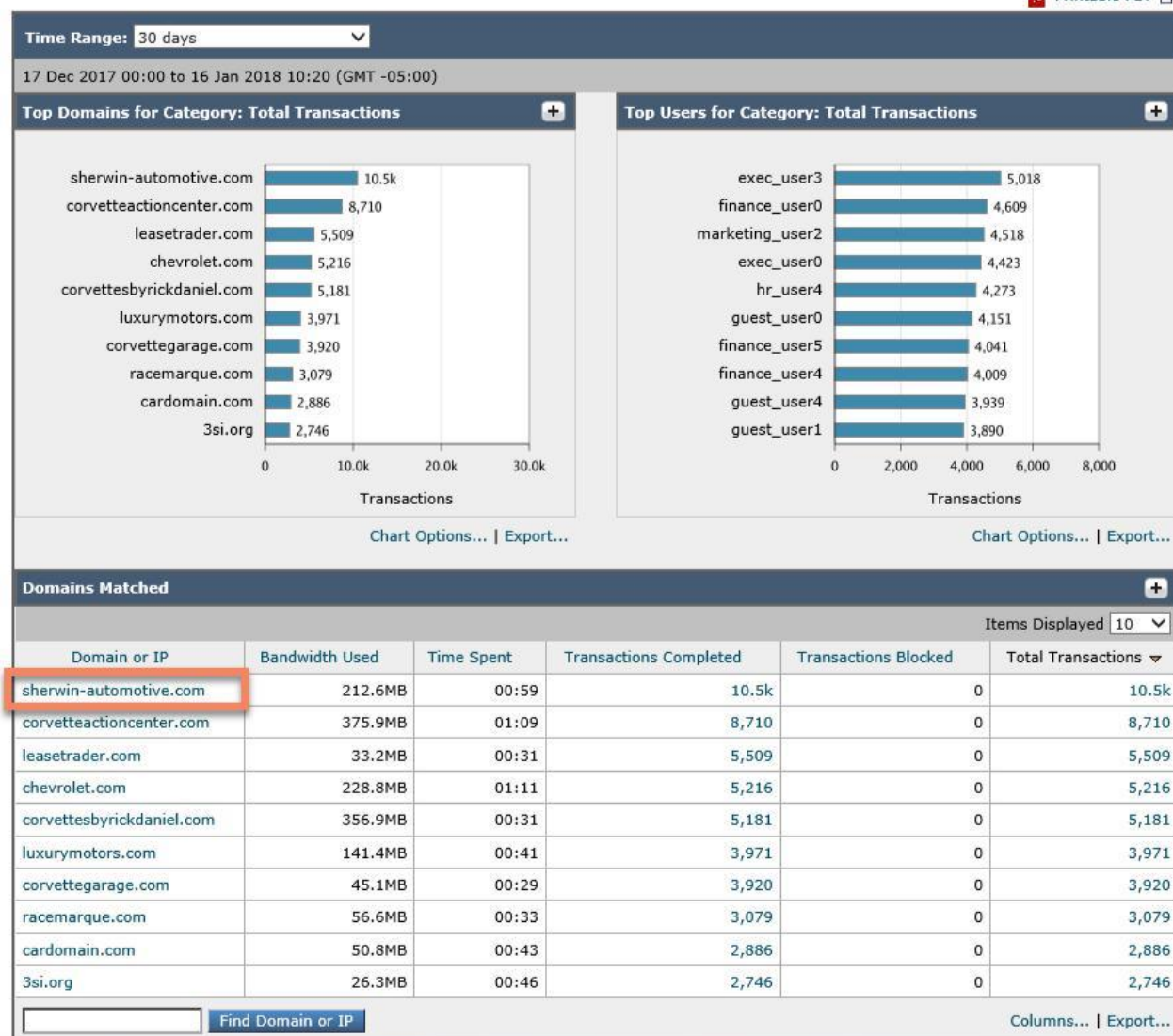
4. [一致した URL カテゴリ] までスクロール ダウンし、[運輸 (Transportation)] カテゴリをクリックします。

marketing_user2	9.9MB	00:01	498	0	498
Find User ID or Client IP Columns... Export...					
URL Categories Matched +					
URL Category	Bandwidth Used	Time Spent	Transactions Completed	Transactions Blocked	Total Transactions
Transportation	212.6MB	00:59	10.5k	0	10.5k
Find URL Category Columns... Export...					

5. このカテゴリに一致するドメインの詳細レポートが表示されます。トランザクションのレポートでは、Sherwin Automotive が上位のドメインとなっていることが確認できます。

URL Categories : Transportation

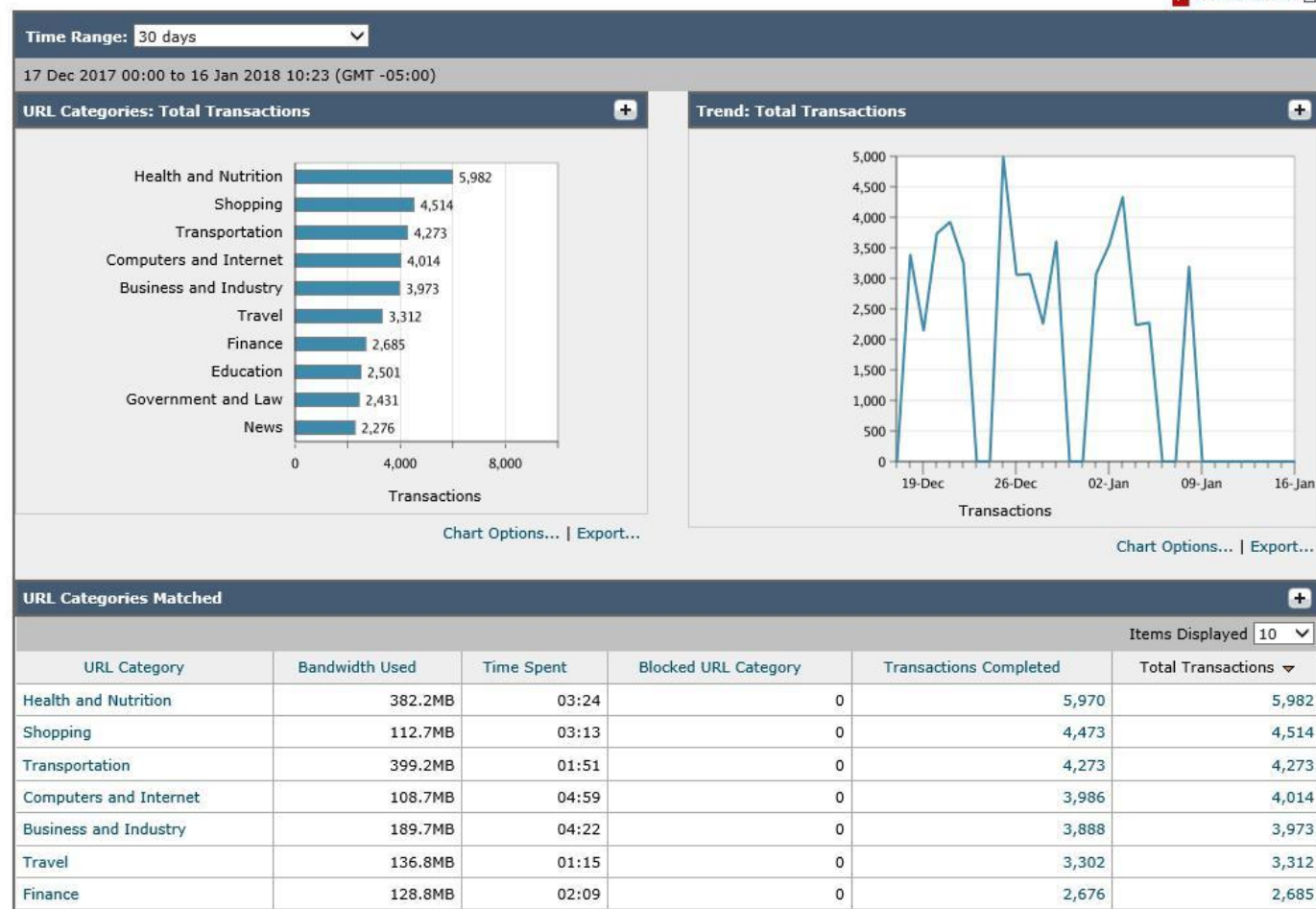
Printable PDF



6. [Web ユーザ (Web Users)] セクションまでスクロール ダウンし、ユーザ名をクリックします。このレポートには、上位カテゴリ、上位ドメイン、一致したアプリケーション、AMP およびマルウェア脅威、使用ポリシーなど、ユーザの行動に関する詳細が表示されます。

Users > **hr_user4@dCloud.cisco.com**

Printable PDF



7. スクロール ダウンして、このレポートには、Cisco AMP エンジンからの脅威情報や検出されたマルウェア脅威も表示されることを示します。WSA は、サポート対象のすべてのマルウェア エンジンで有効になっており、AMP と統合されています。

Advanced Malware Protection Threats Detected

Malware Threat File SHA256	Threat Name	File Type	Transactions Monitored	Transactions Blocked	Transactions Detected
bb4177de...12cdd69d	W32.BB4177DEA9-95.SBX.TG	application/x-dosexec	14	14	28
ea44e077...db44f2d2	W32.Trojan.NM	application/x-dosexec	5	5	10
Totals (all available data):	--	--	19	19	38

Find Malware Threat File SHA256

Malware Threats Detected

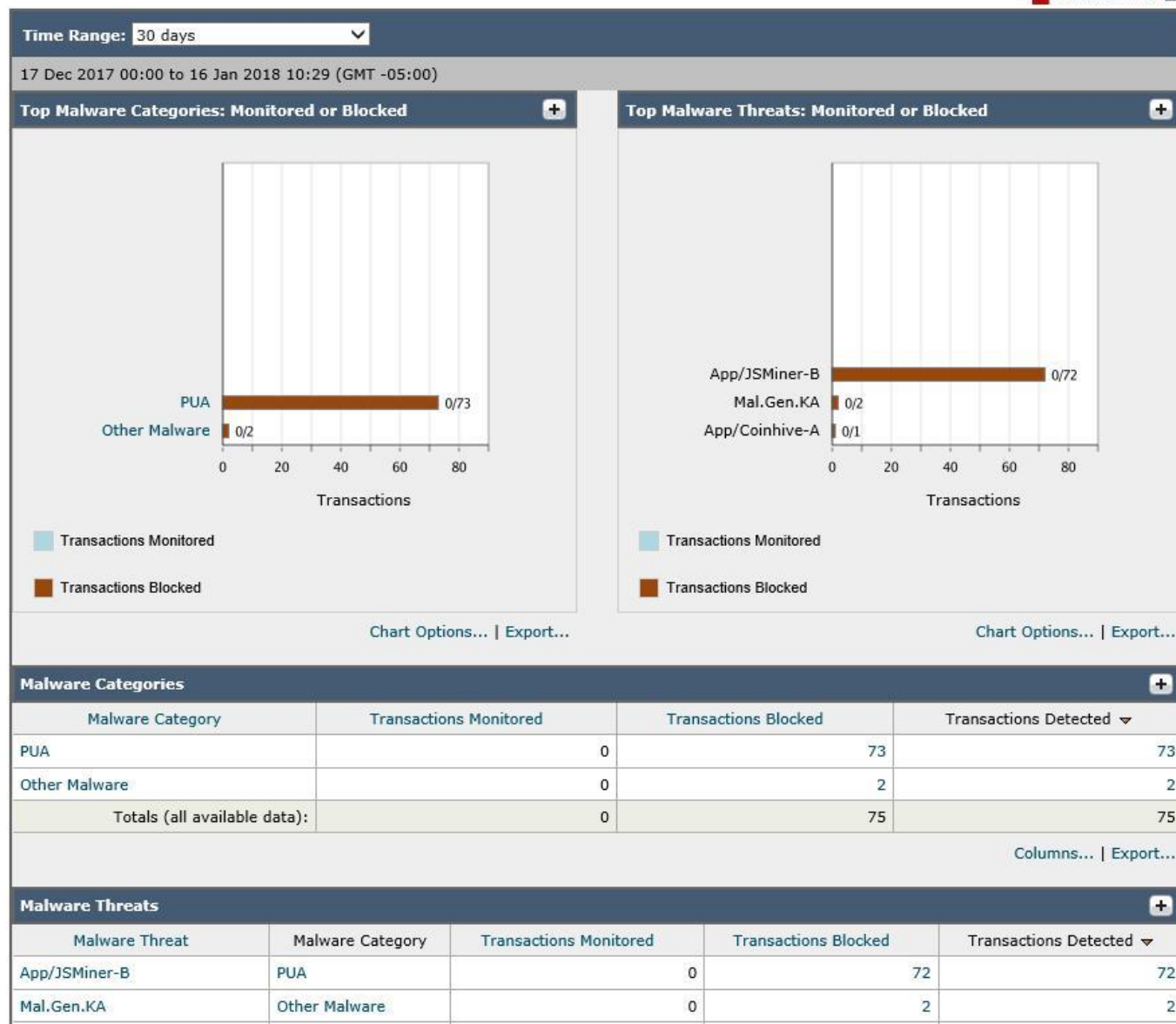
Malware Threat	Malware Category	Bandwidth Saved by Blocking	Transactions Monitored	Transactions Blocked	Total Malware Transactions Detected
App/JSMiner-B	PUA	24.0KB	0	2	2
Totals (all available data):	--	24.0KB	0	2	2

Find Malware Threat

8. メニューから [レポート(Reporting)] > [マルウェア対策 (Anti Malware)] を選択します。このレポートにはマルウェア対策の統計情報が表示されます。ブロックされたマルウェアや監視されたマルウェアなどが確認できます。

Anti-Malware

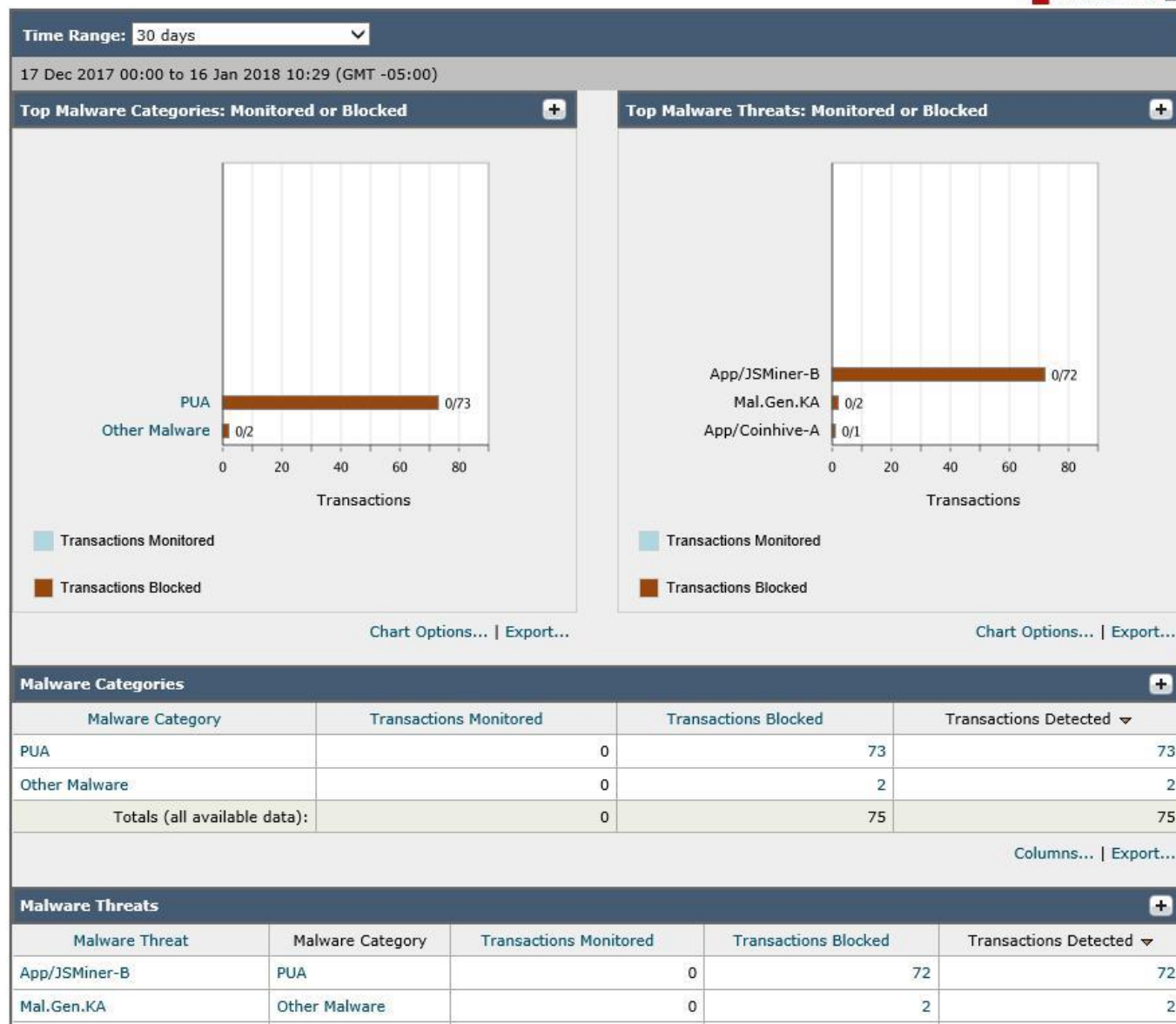
Printable PDF 



9. マルウェアの一覧の中から、脅威を1つクリックします。このレポートには、時間範囲やリスクのあるクライアントを含む、脅威に関する詳細が表示されます。

Anti-Malware

Printable PDF 

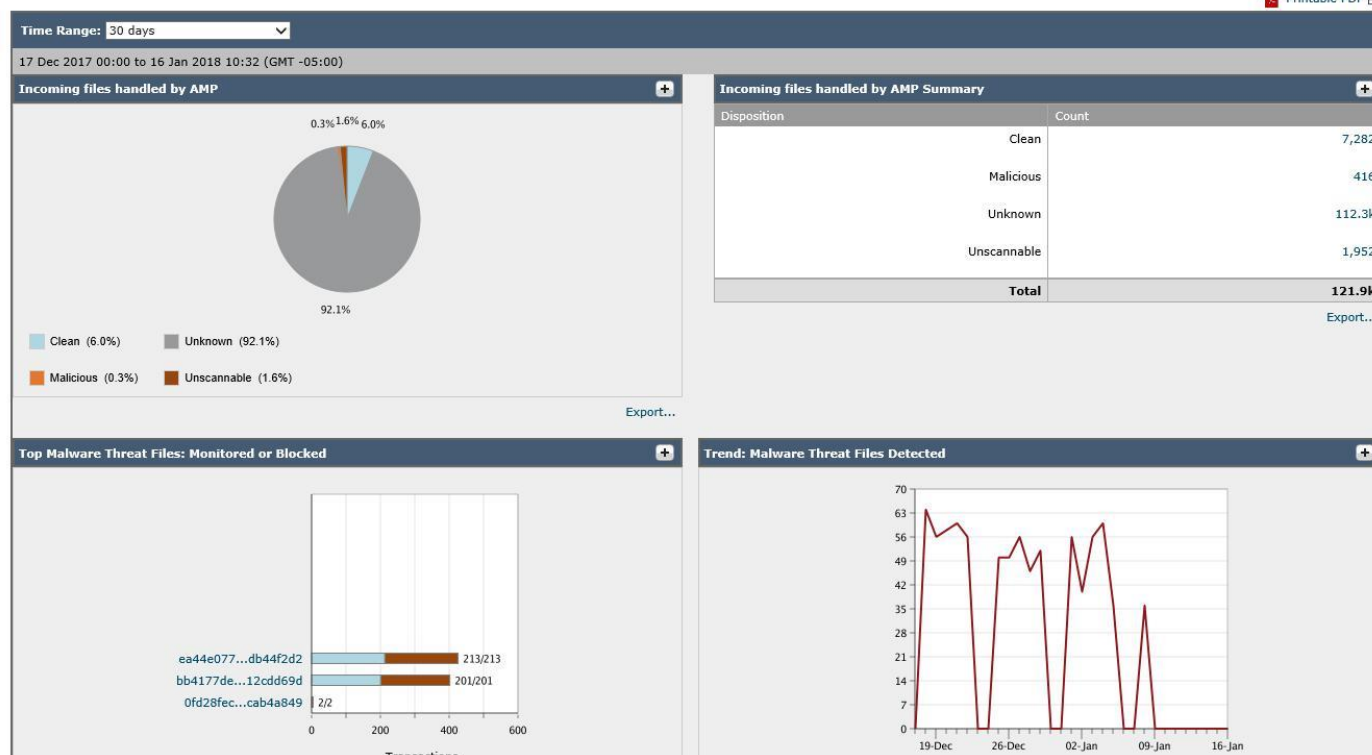


10. メニューから [レポート(Reporting)] > [高度なマルウェア防御(Advanced Malware Protection)] を選択します。このレポートには、AMP によって捕捉/スキャンされた脅威の詳細が表示されます。

Advanced Malware Protection

[Click here to view reports prior to AsyncOS 10.0](#)

Printable PDF



11. [マルウェア脅威ファイル(Malware Threat Files)] までスクロール ダウンします。特定の脅威に関する情報が表示されます。

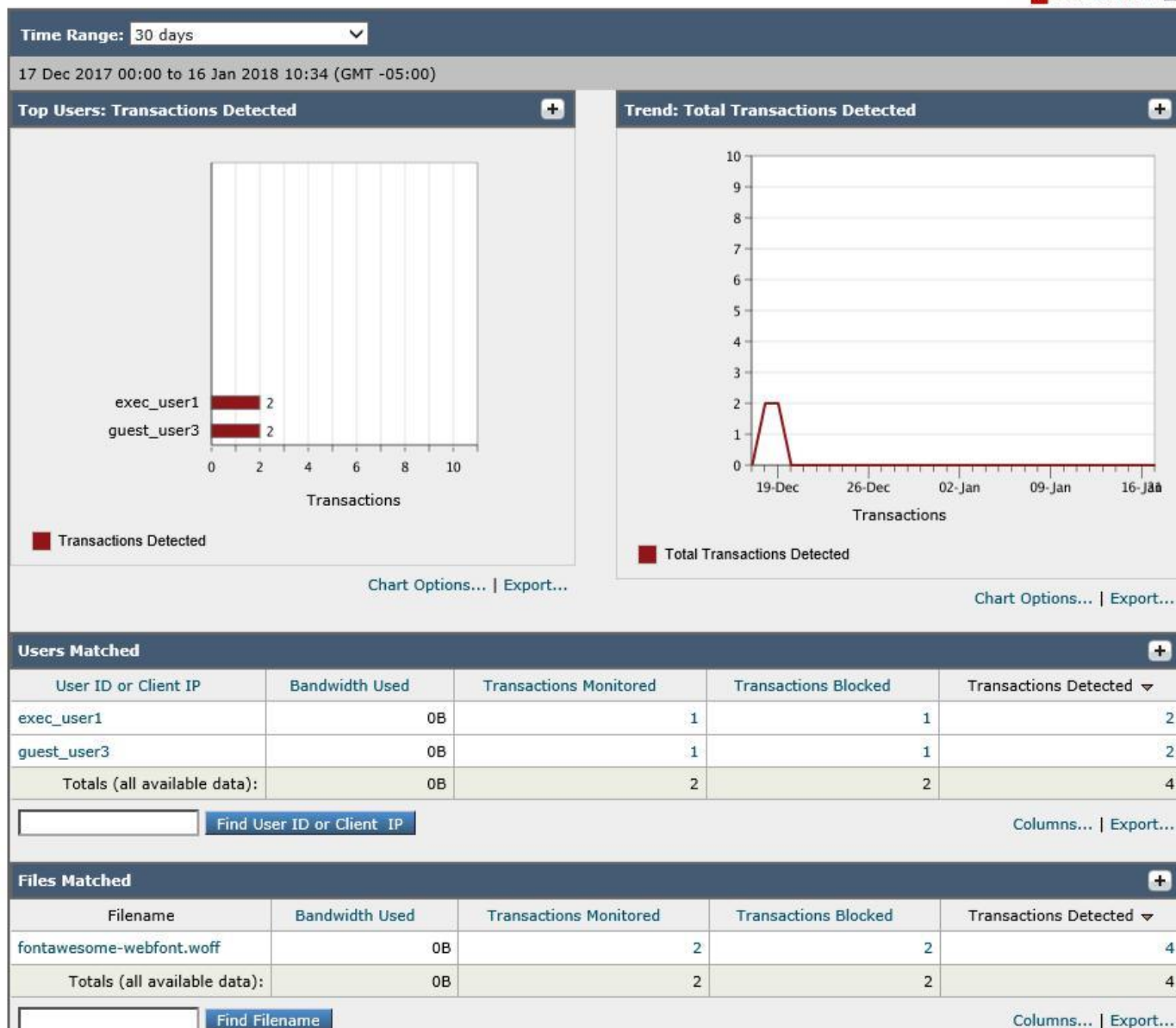
Malware Threat File SHA256	File Names	Threat Name	File Type	Transactions Monitored	Transactions Blocked	Transactions Detected
0fd28fec...cab4a849	fontawesome-webfont.woff	W32.Auto:0fd28fece9.in05.Talos	application/octet-stream	2	2	4
ea44e077...db44f2d2	25296-677636-winzip.exe	W32.Trojan.NM	application/x-dosexec	213	213	426
bb4177de...12cdd69d	FreeRARExtractorElite.exe	W32.BB4177DEA9-95.SBX.TG	application/x-dosexec	201	201	402
Totals (all available data):	--	--	--	416	416	832

Columns... | Export...

12. SHA ファイルのいずれかをクリックします。このレポートには、ダウンロードされた後にブロックされたファイルの名前が表示されます。

Malware Threat Files > SHA256 0fd28fec...cab4a849

 Printable PDF 



13. [詳細(More Details)] セクションまでスクロールダウンしてリンクをクリックすると、**Web トラッキング**に関する詳細を確認できます。

Files Matched +				
Filename	Bandwidth Used	Transactions Monitored	Transactions Blocked	Transactions Detected ▼
fontawesome-webfont.woff	0B	2	2	4
Totals (all available data):		2	2	4

Find Filename Columns... | Export...

More Details on this threat file	
All transactions for this threat:	Web Tracking for SHA256 0fd28fece9ebd606b8b071460ebd3fc2ed7bc7a66ef91c8834f11dfacab4a849
File Analysis details:	File Reputation and Analysis Report

14. 複数のカテゴリを指定して、Web トラッキングの詳細をフィルタリングできます。

Web Tracking

Search

Proxy Services | L4 Traffic Monitor | SOCKS Proxy

Available: 01 Sep 2017 08:15 to 08 Jan 2018 16:59 (GMT -05:00)

Time Range: Custom Range... ▼ 01 Sep 2017 08:00 through 16 Jan 2018 10:34 (GMT -05:00)

User/Client IPv4 or IPv6: (e.g. jdoe, DOMAIN\jdoe, 10.1.1.0, or 2001:420:80:1::5)

Website: (e.g. google.com)

Transaction Type: All Transactions ▼

Advanced *Current Criteria:* File SHA256: 0fd28fece9ebd606b8b071460ebd3fc2ed7bc7a66ef91c8834f11dfacab4a849.

URL Category: Disable Filter
 Filter by URL Category:

Application: Disable Filter
 Filter by Application: (ex. Yahoo Messenger)
 Filter by Application Type: (ex. Instant Messaging)

Policy: Disable Filter
 Filter by Policy:

Advanced Malware Protection: Disable Filter
 Filter by Filename: (ex.avmWin32Lib.jar)
 Disable Filter
 Filter by File SHA256: 0fd28fece9ebd606b8b0 (ex.c44c8f1e50f7d8cceb483e45f4e5f4e071e2a6408893bb109587ea3c2f0f5c58200f)
 Disable Filter
 Filter by AMP File Verdict:

15. [詳細 (More Details)] セクションに戻り、[ファイルレピュテーションと分析レポート (File Reputation and Analysis Report)] をクリックします。

Files Matched +					
Filename	Bandwidth Used	Transactions Monitored	Transactions Blocked	Transactions Detected ▾	
fontawesome-webfont.woff	0B	2	2	4	
Totals (all available data):		0B	2	2	4

[Find Filename](#) [Columns...](#) | [Export...](#)

More Details on this threat file	
All transactions for this threat:	Web Tracking for SHA256 0fd28feca9ebd606b8b071460ebd3fc2ed7bc7a66ef91c8834f11dfacab4a849
File Analysis details:	File Reputation and Analysis Report

注: ブロックされた対象や WSA に送信された対象によっては、情報がすぐに表示されない場合があります。これは、レピュテーションによって即座にブロックされたり、分析が実行中であったりするためです。

File Analysis Detail > 0fd28fec...cab4a849

 [Printable PDF](#)

File Reputation Summary			
17 Dec 2017 00:00 to 16 Jan 2018 10:42 (GMT -05:00)			
File Name	Reputation Score	Disposition	Reputation Verdict Time
fontawesome-webfont.woff	0	Malware	Mon Dec 18 10:29:03 2017
			Export...

File Analysis Summary
General Information
<i>No data found</i>
Behavioural Indicators
<i>No data found</i>

16. メニューから [レポート (Reporting)] > [Webトラッキング (Web Tracking)] を選択します。検索ボックスを使用して、[Web サイト (Website)] に、「Cisco.com」と入力します。[時間範囲 (Time Range)] を [30 日間 (30 days)] に設定します。[検索 (Search)] をクリックします。

Web Tracking

Search

Proxy Services L4 Traffic Monitor SOCKS Proxy

Available: 01 Sep 2017 08:15 to 08 Jan 2018 16:59 (GMT -05:00)

Time Range: 30 days

User/Client IPv4 or IPv6: (e.g. jdoe, DOMAIN\jdoe, 10.1.1.0, or 2001:420:80:1::5)

Website: cisco.com (e.g. google.com)

Transaction Type: All Transactions

Advanced Search transactions using advanced criteria.

Cancel Search

17. ドメインに一致するすべてのサイトについて、判定結果、使用帯域幅、アクセス ユーザなどが表示されます。

Web Tracking

Search

Proxy Services L4 Traffic Monitor SOCKS Proxy

Available: 01 Sep 2017 08:15 to 08 Jan 2018 16:59 (GMT -05:00)

Time Range: 30 days

User/Client IPv4 or IPv6: (e.g. jdoe, DOMAIN\jdoe, 10.1.1.0, or 2001:420:80:1::5)

Website: (e.g. google.com)

Transaction Type: All Transactions

Advanced Search transactions using advanced criteria.

Clear Search

Generated: 16 Jan 2018 10:48 (GMT -05:00)

Printable Download

Results					
Items Displayed 50					
Displaying 1 - 50 of 226 items. « Previous 1 2 3 4 5 Next »					
Time (GMT -05:00)	Website (count)	Display All Details...	Disposition	Bandwidth	User / Client IP
08 Jan 2018 16:00:38	tunnel://www.cisco.com:443 (79)		Allow	3.3MB	exec_user3 198.19.10.203
08 Jan 2018 16:00:38	http://www.cisco.com		Monitor	1,056B	exec_user3 198.19.10.203
08 Jan 2018 14:27:32	tunnel://www.cisco.com:443 (2)		Allow	44.1KB	finance_user3 198.19.10.221
08 Jan 2018 14:27:32	http://www.cisco.com		Monitor	1,123B	finance_user3 198.19.10.221
08 Jan 2018 13:51:19	tunnel://www.cisco.com:443 (2)		Allow	45.0KB	finance_user2 198.19.10.220
08 Jan 2018 13:51:19	http://www.cisco.com		Monitor	1,095B	finance_user2 198.19.10.220
08 Jan 2018 13:02:44	http://www.cisco.com		Monitor	1,106B	guest_user5 198.19.10.229
08 Jan 2018 13:02:44	tunnel://www.cisco.com:443 (2)		Allow	44.0KB	guest_user5 198.19.10.229
08 Jan 2018 12:07:56	http://www-china.cisco.com		Monitor	881B	hr_user3 198.19.10.209
08 Jan 2018 12:01:59	tunnel://www.cisco.com:443 (57)		Allow	2.1MB	finance_user0 198.19.10.218
08 Jan 2018 12:01:57	tunnel://www.cisco.com:443 (21)		Allow	1,001.1KB	finance_user0 198.19.10.218
08 Jan 2018 12:01:56	tunnel://www.cisco.com:443		Allow	66.4KB	finance_user0 198.19.10.218
08 Jan 2018 11:52:36	tunnel://www.cisco.com:443 (79)		Allow	3.1MB	finance_user3 198.19.10.221
08 Jan 2018 11:52:35	http://www.cisco.com		Monitor	1,060B	finance_user3 198.19.10.221
08 Jan 2018 10:27:23	http://www-europe.cisco.com		Monitor	898B	quest_user3 198.19.10.227

© 2018 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(1502R)

この資料の記載内容は 2018 年 3 月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107 - 6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先