FireSIGHT システムでの URL フィルタリングに 関する問題のトラブルシューティング

内容

概要 URLフィルタリングルックアッププロセス クラウド接続の問題 ステップ1: ライセンスの確認 ライセンスがインストールされているか ライセンスの期限が切れていますか。 ステップ2:ヘルスアラートの確認 ステップ 3:DNS設定の確認 ステップ4:必要なポートへの接続の確認 アクセス制御と誤分類の問題 問題1:レピュテーションレベルが選択されていないURLは許可/ブロックされる ルールアクションは許可です <u>ルールアク</u>ションがブロック URL選択マトリックス 問題2:アクセス制御規則でワイルドカードが機能しない 問題 3: URLカテゴリとレピュテーションが入力されていない 関連情報

概要

このドキュメントでは、URL フィルタリングに関連する一般的な問題について説明します。 FireSIGHT Management CenterのURLフィルタリング機能は、監視対象ホストのトラフィックを 分類し、レピュテーションに基づいてアクセスコントロールルールに条件を記述できるようにし ます。

URLフィルタリングルックアッププロセス

URLルックアッププロセスを高速化するために、URLフィルタリングはFirepowerシステムにロー カルにインストールされたデータセットを提供します。アプライアンスで使用可能なメモリ (RAM)の量に応じて、次の2種類のデータセットがあります。

データセットのタイプ *ブーション5.3 バージョン5.4以降* 2,000万のURLデータセット >2 GB >3.4 GB 100万のURLデータセット <= 2 GB 3.4 GB未満



クラウド接続の問題

ステップ1: ライセンスの確認

ライセンスがインストールされているか

URLフィルタリングライセンスなしで、カテゴリとレピュテーションベースのURL条件をアクセ スコントロールルールに追加できますが、最初にURLフィルタリングライセンスをFireSIGHT Management Centerに追加し、ポリシーの対象となるデバイスで有効にするまで、アクセスコン トロールポリシーを適用できません。

ライセンスの期限が切れていますか。

URL フィルタリング ライセンスが期限切れになると、カテゴリおよびレピュテーション ベース の URL 条件を持つアクセス コントロール ルールは URL のフィルタリングを停止し、FireSIGHT 管理センターはクラウド サービスにコンタクトしなくなります。

ヒント:FireSIGHTシステムでURLフィルタリング機能を有効にし、管理対象デバイスに URLフィルタリングライセンスを適用する方法については、『<u>FireSIGHTシステムでの</u> <u>URLフィルタリングの設定例</u>』を参照してください。

ステップ2:ヘルスアラートの確認

URL Filtering Monitorモジュールは、FireSIGHT Management Centerとシスコのクラウド間の通 信を追跡します。システムは、よくアクセスするURLのURLフィルタリング(カテゴリおよびレ ピュテーション)データを取得します。URLフィルタリングモニタモジュールは、FireSIGHT Management Centerと、URLフィルタリングを有効にした管理対象デバイス間の通信も追跡しま す。

URLフィルタリングモニタモジュールを有効にするには、Health Policy Configurationページに移動し、URL Filtering Monitorを選択します。モジュールをヘルスステータステストで使用できるようにするには、[Enabled] オプションの[On] オプションボタンをクリックします。設定を有効にするには、FireSIGHT Management Centerに正常性ポリシーを適用する必要があります。

Description URL Filtering Monitor

Enabled

 On Off

- Critical Alert: FireSIGHT Management Centerがクラウドと正常に通信できない場合、または クラウドから更新を取得できない場合、そのモジュールのステータス分類はCriticalに変わり ます。

ステップ3:DNS設定の確認

FireSIGHT Management Centerは、クラウドのルックアップ中にこれらのサーバと通信します。

database.brightcloud.com

service.brightcloud.com

ファイアウォールで両方のサーバが許可されていることを確認したら、FireSIGHT Management Centerで次のコマンドを実行し、Management Centerが名前を解決できるかどうかを確認します admin@FireSIGHT:~\$ sudo nslookup database.brightcloud.com

admin@FireSIGHT:~\$ sudo nslookup service.brightcloud.com

ステップ4:必要なポートへの接続の確認

FireSIGHTシステムは、クラウドサービスとの通信にポート443/HTTPSおよび80/HTTPを使用します。

Management Centerが正常にnslookupを実行できることを確認したら、telnetを使用してポート 80とポート443への接続を確認します。URLデータベースはdatabase.brightcloud.comのポート 443でダウンロードされますが、不明なURLクエリはservice.brightcloud.comのポート80で実行さ れます。

telnet database.brightcloud.com 443 telnet service.brightcloud.com 80 次に、database.brightcloud.comへのtelnet接続が成功した例を示します。

Connected to database.brightcloud.com. Escape character is '^]'.

アクセス制御と誤分類の問題

問題1: レピュテーションレベルが選択されていないURLは許可/ブロックされる

URLが許可またはブロックされているのに、アクセスコントロールルールでそのURLのレピュテ ーションレベルを選択していない場合は、このセクションを読んで、URLフィルタリングルール の動作を理解してください。

ルールアクションは許可です

レピュテーションレベルに基づいてトラフィックを許可するルールを作成する場合、レピュテー ションレベルを選択すると、最初に選択したレベルよりも安全性の低いレピュテーションレベル もすべて選択されます。たとえば、セキュリティリスクのある良性サイト(レベル3)を許可する ルールを設定すると、自動的に良性サイト(レベル4)およびよく知られている(レベル5)サイ トも許可されます。 Add Rule

Name Action & Allow IPS:	Enabled no policies Variables: n/a Files: no inspection	Insert into Catego	ory 💌 St	tandard Rules	~
Zones Networks VLAN Tags Users	Applications Ports URLs		Inspection	Logging	Comments
Categories and URLs C ③ Search by name or value Any	Reputations Any S - Well Known		Selected URLs (1) Bot Nets (Reputa	tions 3-5)	ü
 Abortion Abused Drugs Adult and Pornography Alcohol and Tobacco Auctions Bot Nets 	 4 - Benign sites 3 - Benign sites with security risks 2 - Suspicious sites 1 - High Risk 	Add to Rule			
Business and Economy CDNs Cheating			Enter URL	Add	Add

ルールアクションがブロック

レピュテーションレベルに基づいてトラフィックを**ブロック**するルールを作成する場合、レピュ テーションレベルを選択すると、最初に選択したレベルよりも厳しいレピュテーションレベルも すべて選択されます。たとえば、*セキュリティリスクのある良性サイト*(レベル3)をブロックす るルールを設定すると、*疑わしいサイト*(レベル2)および*高リスク*(レベル1)のサイトも自動 的にブロックされます。

Add Rule					?
Name		Insert into Catego	ory 👻	Standard Rules	
Action 🗙 Block 💌 IPS	no policies Variables: n/a Files: no inspectio	on Logging: no l	logging		
Zones Networks VLAN Tags Users	Applications Ports URLs		Inspect	ion Logging	Comments
Categories and URLs 🖸 🛛 🖸	Reputations		Selected URLs (1	L)	
\lhd Search by name or value	🗾 Any		Bot Nets (Re	putations 1-3)	ï
💣 Any	🚽 5 - Well Known				
Abortion	🚽 4 - Benign sites				
Abused Drugs	🧾 3 - Benign sites with security risks				
Adult and Pornography	2 - Suspicious sites	Add to Rule			
Alcohol and Tobacco	🧾 1 - High Risk				
Auctions					
Bot Nets					
Business and Economy					
CDNs					
Cheating			Enter URL		Add
Cheating			Enter URL	Add	Canc

URL選択マトリックス

選択したレピュテーションレベル	選択した 高リスク	ルールアクシ 不審なサイト	ョン · セキュリティリスクのある良性サイト	良
1-高リスク				
2-疑わしいサイト	Block			
3 – セキュリティリスクのある良性サ イト	Block	Block		
4 – 良性サイト	Block	Block	Block	
5-よく知られている	Block	Block	Block	Blo

問題2:アクセス制御規則でワイルドカードが機能しない

FireSIGHTシステムは、URL条件でのワイルドカードの指定をサポートしていません。この状態 は、cisco.comで警告に失敗する可能性があります。

cisco.com

また、不完全なURLが他のトラフィックと一致する場合も、望ましくない結果を引き起こします 。URL条件で個々のURLを指定する場合は、影響を受ける可能性がある他のトラフィックを慎重 に考慮する必要があります。たとえば、cisco.comを明示的にブロックするシナリオを考えてみま す。ただし、部分文字列の照合は、cisco.comをブロックするとsanfrancisco.comもブロックされ ることを意味します。これは意図していない可能性があります。

URLを入力するときは、ドメイン名を入力し、サブドメイン情報を省略します。たとえば、 <u>www.cisco.com</u>ではなくcisco.comと入力します。 <u>Allow</u>ルールでcisco.comを使用する場合、ユー ザは次のURLのいずれかを参照できます。

http://cisco.com
http://cisco.com/newcisco
http://www.cisco.com

問題 3: URLカテゴリとレピュテーションが入力されていない

URLがローカルデータベース内になく、そのURLがトラフィック内で初めて見られる場合は、カ テゴリまたはレピュテーションが設定されていない可能性があります。これは、未知のURLが初 めて見られたときに、ACルールと一致しないことを意味します。一般的にアクセスされる URLのURLルックアップは、最初にURLが表示されたときに解決しないことがあります。この問 題は、バージョン5.3.0.3、5.3.1.2、および5.4.0.2、5.4.1.1で修正されています。

関連情報

・<u>FireSIGHTシステムでのURLフィルタリングの設定</u>

• <u>テクニカル サポートとドキュメント – Cisco Systems</u>