

Cisco Secure Network Analytics

フローセンサーとロードバランサの統合ガイド 7.4.2



目次

はじめに	3
対象読者	3
はじめる前に	3
ロード バランサの設定	4
HTTP の XFF オプションの無効化	4
[iRuleの作成(Creating the iRule)]	5
仮想サーバーのリソースとしての iRule の追加	8
ネットワーク内のすべてのロードバランサの設定	9
FlowSensor での XFF 処理の有効化	10
設定の確認	11
Stealthwatch デスクトップクライアントの設定の確認	11
フローテーブルへの列の追加(デスクトップクライアント)	11
Stealthwatch Web アプリケーションの設定の確認	12
サポートへの問い合わせ	13

はじめに

ロードバランサがネットワーク上のリソースの前にインストールされている場合、可視性が不明瞭になり、Stealthwatchシステムでの脅威の検出が低下する可能性があります。

ロードバランサとFlowSensorを設定するには、このガイドの手順を使用します。この設定によって、 クライアント側とサーバー側のフローが一緒にスティッチングされるため、外部ホストは内部ホストに 接続し、フローセンサーとStealthwatchシステムで可視性と強化されたセキュリティを提供できま す。

v7.4.0 では、Cisco Stealthwatch Enterprise 製品のブランド名を Cisco Secure Network Analytics に変更しました。詳細なリストについては、<u>リリースノート</u>を参照してください。こ のガイドでは、以前の製品名である Stealthwatch が必要に応じて明確さを維持するため に使用され、Stealthwatch Management Console や SMC などの用語も使用されていま す。

対象読者

このガイドの主な対象者には、Stealthwatchシステムの設定を担当する管理者が含まれています。

はじめる前に

このガイドの手順を開始する前に、次の手順を実行する必要があります。

- Stealthwatchシステムが通信していることを確認します。Stealthwatchデスクトップクライアントに移動します。アラームテーブルを確認し、アクティブな[管理チャネルダウン(Management Channel Down)]アラームまたは[フェールオーバーチャネルダウン(Failover Channel Down)]アラームがないことを確認します。
- Stealthwatch システムアプライアンスのライセンスがアクティブであることを確認します。

ロード バランサの設定

ロードバランサを設定するには、次の手順を使用します。HTTPの場合は、X-Forwarded-For(XFF) オプションを無効にし、iRuleを作成して、仮想サーバーのリソースを有効にします。既存の iRuleを 使用する場合は、ここに記載されている情報を使用して変更できます。正常に統合するには、この セクションの手順をネットワーク内のすべてのロードバランサに適用します。

このガイドの手順では、例として F5 ロードバランサの設定を示していますが、この設定はすべての タイプのロードバランサで使用できます。

HTTPの XFF オプションの無効化

HTTPのXFFオプションを無効にするには、次の手順を使用します。

XFF HTTP ヘッダーにデータを挿入するための組み込み機能は、次の手順に従い F5 ロードバラン サで無効にする必要があります。

- 1. F5 ロードバランサ設定ユーティリティにログインします。
- 2. [メイン(Main)] タブで、[ローカルトラフィック(Local Traffic)] をクリックします。
- 3. [プロファイル(Profiles)]>[サービス(Services)]>[HTTP]の順にクリックします。

[サービス(Services)]メニューに HTTP が表示されない場合は、ステップ8に進みます。

6	ONLINE (ACTIVE Standalone	E)			
Main	Help	About	Local Traffic » Profiles : Services : HTTP		
Maga Sta	tistics		🗱 🔹 Services 🔹 Content 🔹 Databases 🔹 Persistence Protocol 🔹 SSL 🔹 Authentication 🔹 Messe	ge Routing 👻 Oth	er 👻
iAp	ps		× Search		Create
S DN	s		Applicat Applicat	on Parent Profile	Partition / Path
	al Traffic		L http	(none)	Common
			http-explicit	(none)	Common
	Network Map		L http-transparent P0	(none)	Common
	Virtual Servers	Þ	Delete		
	Policies	×.			
	Profiles	÷			
	iRules	÷			
	Pools	Þ			
	Nodes	Þ			
	Monitors	(\Rightarrow)			
	Traffic Class	(\Rightarrow)			
	Address Translation	Þ			
Ac	celeration				

- 4. [http]をクリックします。
- 5. [設定(Settngs)]で[X-Forwarded-Forの挿入(Insert X-Forwarded-For)]を見つけます。
- 6. ドロップダウンリストから[無効(Disabled)]を選択します(または、[有効(Enabled)]チェック ボックスをオフにしてクリアします)。

Settings		^
Basic Auth Realm		
Fallback Host		
Fallback on Error Codes		
Request Header Erase		
Request Header Insert		
Response Headers Allowed		
Request Chunking	Preserve V	
Response Chunking		i
OneConnect Transformations	D Enabled	4
Redirect Rewrite	None 🔽	
Encrypt Cookies		
Cookie Encryption Passphrase		
Confirm Cookie Encryption Passphrase		
Insert X-Forwarded-For	Disabled V	:
LWS Maximum Columns	80	
LWS Separator		

- 7. [更新(Update)] ボタンをクリックします。
- 8. [サービス(Services)]メニューから、[高速 HTTP(Fast HTTP)]をクリックします。

[サービス(Services)]メニューに[高速HTTP(Fast HTTP)]がない場合は、このセクションの残りの 手順をスキップします。[iRuleの作成(Creating the iRule)]に進みます。

- 9. [X-Forwarded-Forの挿入(Insert X-Forwarded-For)]を見つけます。
- 10. ドロップダウンリストから[無効(Disabled)]を選択します(または、[有効(Enabled)]チェック ボックスをオフにしてクリアします)。
- 11. [更新(Update)] ボタンをクリックして、保存して終了します。
- 12. [iRuleの作成(Creating the iRule)]に進みます。

[iRuleの作成(Creating the iRule)]

XFF ヘッダーの iRule を追加するには、次の手順を使用します。この手順は、ロードバランサの IP アドレスをマッピングし、正確なポートおよびプロトコル情報を FlowSensor に報告するために使用し ます。

既存の iRule を使用する場合は、ここに記載されている情報を使用して変更できます。

F5 ロードバランサで XFF ヘッダーの iRule を作成するには、次の手順を実行します。

- 1. [メイン(Main)] タブで、[ローカルトラフィック(Local Traffic)] をクリックします。
- 2. [iRules] をクリックします。
- 3. [Create] ボタンをクリックします。

CONLINE (ACTIVE)							
Main Help Abo	ut	Local Traffic » iRules : iRule List					
Statistics		🐲 🚽 iRule List Data Group List	iFile List Statistics				
iApps		*Se	arch				Create
S DNS		Name A		Verification		Certificate Application	a 🌣 Partition / Path
~		Sys_APM_ExchangeSupport_OA_BasicA	uth	F5 Verified		f5-irule	Common
Local Traffic		sys_APM_ExchangeSupport_OA_NtlmAuth		F5 Verified	E F5 Verified		Common
Network Map		sys_APM_ExchangeSupport_helper		F5 Verified	3	f5-irule	Common
Virtual Servers	+	sys_APM_ExchangeSupport_main		F5 Verified		f5-irule	Common
Policies	+	sys_APM_Office365_SAML_BasicAuth		F5 Verified		f5-irule	Common
Profiles	•	sys_APM_activesync		F5 Verified		f5-irule	Common
iRules		sys_auth_krbdelegate		F5 Verified		f5-irule	Common
Pools		□ _sys_auth_idap		P] F5 Verified		f5-irule	Common
Nadas		sys_auth_radius		E5 Verified		f5-irule	Common
Nodes	<u>,</u>	sys_auth_ssl_cc_ldap		E5 Verified		f5-irule	Common
Monitors	0	Add Signature Add Checksum Delete]			P	'age 1 of 2 🔽 🕨
Traffic Class	 (*) 						
Address Translation							

4. [名前(Name)]フィールドに、「xff」と入力します。

Hostname: bigip1. IP Address: 1014	.com 0	Date: Jun 12, 2017 User: a Time: 10:56 AM (EDT) Role: A	lmin Iministrator			
ONLINE (A	\СТІVЕ) е					
Main Help	About	Local Traffic » iRules : iRule	List » New iRule			
Matistics						
-		Properties				
iApps		Name	xff			
S DNS			1			
Local Traffic						
Network Map						
Virtual Servers						
Policies) E					
Profiles	بالمتسمر					

続行…

```
5. 次のテキストをコピーして、[定義(Definition)]フィールドに貼り付けます。
when CLIENT_ACCEPTED {
 if { [PROFILE::exists clientssl] } then {
   set client_protocol "https"
   set local_port 443
 }else{
   set client protocol "http"
   set local_port 80
 }
}
when HTTP_REQUEST {
 if { [HTTP::header exists "X-Forwarded-For"] } {
   HTTP::header replace X-Forwarded-For "[HTTP::header X-Forwarded-For], [IP::client_addr]"
 }else{
   HTTP::header insert "X-Forwarded-For" [IP::client_addr]
 }
 if { [HTTP::header exists "X-Forwarded-Proto"] } {
   HTTP::header replace X-Forwarded-Proto "[HTTP::header X-Forwarded-Proto], $client_protocol"
 }else{
   HTTP::header insert "X-Forwarded-Proto" $client protocol
 }
 if { [HTTP::header exists "X-Forwarded-Port"] } {
   HTTP::header replace X-Forwarded-Port "[HTTP::header X-Forwarded-Port], [TCP::client_port]"
 }else{
   HTTP::header insert "X-Forwarded-Port" [TCP::client_port]
 }
 if { [HTTP::header exists "X-Forwarded-Host"] } {
   HTTP::header replace X-Forwarded-Host "[HTTP::header X-Forwarded-Host], [IP::local_addr]:$local_port"
 }else{
   HTTP::header insert "X-Forwarded-Host" [IP::local_addr]:$local_port
 }
}
    6. 「終了 (Finished)] ボタンをクリックして、保存して終了します。
```

7.「仮想サーバーのリソースとしての iRule の追加」に進みます。

仮想サーバーのリソースとしての iRule の追加

仮想サーバーを有効にするには、新しい XFF iRule を F5 ロードバランサのリソースとして追加する 必要があります。この手順により、ロードバランサが XFF ヘッダーを報告できるようになります。

- 1. [メイン(Main)] タブで、[ローカルトラフィック(Local Traffic)] をクリックします。
- 2. [仮想サーバー(Virtual Servers)]をクリックします。
- 3. [サービスポート(Service Port)]を検索し、デバイスで処理されるトラフィックを処理している サービスポート 80(HTTP)または 443(HTTPS)を見つけます。[仮想サーバー名(Virtual Server Name)]をクリックします。

Main Help About	Local Traffic » Virtual Servers : Virtual Server List							
Mag Statistics	Image: Server List Virtual Address List Statistics	•						
іАрря	* Search							Create
S DNS	V Status A Name	Description	Application	Destination	Service Port	Ф Туре	Resources	Partition / Path
Real Local Traffic	internal-outbound		An	y IPv4	0 (Any)	Forwarding (IP)	Edit	Common
Local frame	web_server_1-ssh-vip		10.	208.1.10	22 (SSH)	Standard	Edit	Common
Network Map	web_server_1-www-vip		2 10.	208.1.10	80 (HTTP)	Standard	Edit	Common
Virtual Servers >	Enable Disable Delete				†			
Policies >								
Profiles								
iRules >								
Pools >								
Nodes >								
Monitors 🕒								
Traffic Class								
Address Translation								
Acceleration								
Device Management								

- 4. [リソース(Resources)] タブをクリックします。
- 5. [IRules] セクションで、[管理(Manage)] ボタンをクリックします。

Main Help About	Local Traffic » Virtual Servers : Virtual Server List » web_server_f-awwwvip
Magazina Statistics	🔅 - Properties Resources Statistics 🗵
iApps	Load Balancing
S DNS	Default Pool web server 1-www V
Local Traffic	Default Persistence Profile None 🔍
Network Map	Falback Persistence Profile None
Virtual Servers	Update
Policies >	Rules Minage
Profiles	Name
iRules >	
Pools >	Manaae
Nodes	Fonces
Monitors 💿	Neneo
Traffic Class	TO (BLORUS KO GRAPH)
Address Translation	
Acceleration	

6. 使用可能な iRules をスクロールして、新しい XFF iRule を見つけます。[XFF iRule] をクリック して選択します。 7. [<<] ボタンをクリックして、[有効(Enabled)] ボックスに XFF iRule を追加します。

ONLINE (ACTIVE) Standalone					
Main Help About	Local Traffic » Virtual Serve	ers : Virtual Serve	er List » web_serve	r_1-www-vip	
Mage Statistics	🔅 🗸 Properties Re	esources	Statistics		
iApps	Resource Management				
S DNS		Enabl	ed	Available	
Local Traffic	iRule	/Common xff	/Cor 	nmon /s_APM_ExchangeSupport_OA_BasicAuth /s_APM_ExchangeSupport_OA_NtImAuth /s_APM_ExchangeSupport_balaer	0
Network Map				/s_APM_ExchangeSupport_main	·
Virtual Servers		Up D	lown		
Policies	Cancel Finished				
Profiles			da		

8. [終了(Finished)] ボタンをクリックして、保存して終了します。

ネットワーク内のすべてのロードバランサの設定

ネットワークに複数のロードバランサが連結されている場合は、「FlowSensorでの XFF 処理の有効 化」に進む前に、「ロードバランサの設定」セクションの前述の手順を各ロードバランサに適用しま す。

各ロードバランサを設定すると、XFF 情報が保持されて付加されます。この設定では、FlowSensor は変換されたホストにある元のロードバランサの IP アドレスのみを報告します。

ロードバランサの設定手順には、次の手順が含まれます。

- <u>HTTP の XFF オプションの無効化</u>
- iRule の作成
- 仮想サーバーのリソースとしての iRule の追加

FlowSensor での XFF 処理の有効化

FlowSensorのXFF ヘッダーフィールドを処理するには、次の手順を実行します。

- 1. StealthWatch Management Console にログインします。
- 2. [構成(Configure)]>[グローバル集中管理(GLOBAL Central Management)]をクリックします。
- 3. フローセンサーの *** ([省略記号(Ellipsis)])アイコンをクリックし、[アプライアンス統計情報 の表示(View Appliance Statistics)]をクリックします。フローセンサーの管理インターフェイ スが開きます。
- 4. [設定(Configuration)]>[詳細設定(Advanced Settings)]をクリックします。
- 5. [X-Forwarded-For処理の有効化(Enable X-Forwarded-For-Processing)] チェックボックス をオンにします。

cisco	FlowSensor VE									
Home	Advanced Settings									
🔑 Configuration 🛛 🖻										
🐣 Manage Users 🛛 🗄	Export Packet Payload									
🖋 Support 🗉	Export Application Identification									
Audit Log	Include IPv6 Include HTTPS Header Data (Applies only to IPFIX exports.)									
🔆 Operations										
► Logout	Include HTTP Header Data (Applies only to IPFIX exports.)									
A Help	Export 32	bytes of the HTTP Request Path.								
	2									
	Enable VXLAN Decapsulation									
	Enable GENEVE Decapsulation									
	Enable X-Forwarded-For Processing									
	Enable ETA Processing									
	Cache Mode									
	Ise single shared cache for all monitoring ports									
	O Use independent caches for each monitoring port									
	Apply									

- 5. [適用(Apply)] ボタンをクリックします。
- 6. ロードバランサのサポートを受けているネットワーク内のすべての FlowSensor で、これらの 手順を繰り返します。
- 7. 「<u>設定の確認</u>」に進みます。

設定の確認

ロードバランサの設定を確認するには、Stealthwatch デスクトップクライアントまたは Stealthwatch Web アプリケーションにログインします。 デスクトップクライアントは、ロードバランサの IP アドレスとポートを提供し、Web クライアントはロードバランサの IP アドレスを提供します。

Stealthwatch デスクトップクライアントの設定の確認

デスクトップクライアントのロードバランサの IP アドレスとポートを確認するには、次の手順を使用します。

- F5 ロードバランサの前にあるクライアント上に X-Forwarded-For トラフィックを生成するには、ロードバランサの背後にある Web サーバーのブラウザを使用して、デスクトップクライアントにログインします。
- 2. [エンタープライズツリー(Enterprise Tree)] で FlowSensor を見つけます。FlowSensor の名 前(または IP アドレス)を右クリックします。
- 3. [7n-(Flow)] > [7n-F-7n(Flow Table)]
- 4. [変換されたホスト(Translated Host)] 列と[変換されたポート(Translated Port)] 列を確認して、F5 ロードバランサの IP アドレスとポートが表示されていることを確認します。
 - 変換されたホスト(ロードバランサの IP アドレス)

			Stearth	watch Managemer	nt Console (admin -			
1 Enterprise	Flow Ta	ble ×						
SMC SUDP Directors	💎 Filter	 Q Domain : Q FlowSensor : f5−c 			• Tim	e : Last 5 minutes		
 Tell Host Groups 	Table	Short List						
Network Devices	Flow Table	Flow Table - 3 records						
🕨 🚧 Maps	Translated	Host 🗢 Translated Por	t 🗘 Client Host 🌲	Server Host		Application 🗘 S		
 FlowCollectors \$ 9 			192.	192.	03:07:35	HTTP (unclassified)		
 Exporters FlowSensors 			192.	192.	03:07:35	SSH/SCP (unclassified)		
F5-c Galaxies	local 10.	52	192	192.	00:00:02	HTTPS (unclassified)		
🙀 External Devices								

• 変換されたポート(ロードバランサのポート)

フローテーブルへの列の追加(デスクトップクライアント)

[変換されたホスト(Translated Host)]列と[変換されたポート(Translated Port)]列がデスクトップク ライアントのフローテーブルに表示されない場合は、次の手順を実行します。

- 1. 任意の列を右クリックします。
- 2. リストをスクロールします。Tの列に到達するまで、[追加(More)]を選択します。
- 3. [変換されたホスト(Translated Host)]と[変換されたポート(Translated Port)]をクリックして、フローテーブルに追加します。

Stealthwatch Web アプリケーションの設定の確認

Web アプリケーションのロードバランサの IP アドレスを確認するには、次の手順を使用します。変換 されたポートは、Web アプリケーションでは使用できません。ポートを確認するには、「<u>SMC デスク</u> トップクライアントの設定の確認」を参照してください。

- 1. (F5 ロードバランサの背後にある) サーバー上の Web ページを開きます。
- 2. SMC にログインします。
- 3. [調査(Investigate)]>[フロー検索(Flow Search)]をクリックします。
- 4. [検索(Search)]をクリックします。
- 5. フロー検索の結果にフローが表示されたら、[列の管理(Manage Columns)]をクリックしま す。
- 6. チェックボックスをオンにして、[ピアNAT(Peer NAT)]と[サブジェクトNAT(Subject NAT)] にチェックマークを追加します。
- 7. [設定(Set)]をクリックします。
- ロードバランサの IP アドレスが [ピアNAT(Peer NAT)] 列または [サブジェクトNAT(Subject NAT)] 列に表示されていることを確認します。
 この列は、フローの方向によって決まります。

Flow	Flow Search Results (10)									
Edit	Edit Search Time Range: Last 5 minutes Subject: Orientation: Either									
	_					_				
	START	DURATION	SUBJECT IP ADDRESS	SUBJECT PORT/PROTOCOL	SUBJECT NAT	SUBJECT HOST GROUPS	SUBJECT BYTES	CONNECTION		
۲	Aug 10, 2017 9:17:40 AM	2m 17s	192 ⊖ View URL Data	52851/TCP	-	Catch All	11.5K	HTTP (unclassified)		
۲	Aug 10, 2017 9:17:40 AM	2m 19s	192. View URL Data	54733/TCP	-	Catch All	9.74K	HTTP (unclassified)		
۲	Aug 10, 2017 9:17:40 AM	2m 17s	192. ⊡ View URL Data	60374/TCP	-	Catch All	9.42K	SSH/SCP (unclassified)		
۲	Aug 10, 2017 9:16:40 AM	17s	192. View URL Data	52851/TCP		Catch All	3.83K	HTTP (unclassified)		
۲	Aug 10, 2017 9:16:40 AM	19s	192 © View URL Data	54733/TCP	-	Catch All	3.25K	HTTP (unclassified)		
۲	Aug 10, 2017 9:17:40 AM	2m 15s	192. ⁻ ⊡ View URL Data	46467/TCP	-	Catch All	7.64K	SSH/SCP (unclassified)		
۲	Aug 10, 2017 9:16:40 AM	17s	192. ⊖ View URL Data	60374/TCP		Catch All	3.14K	SSH/SCP (unclassified)		
۲	Aug 10, 2017 9:16:40 AM	15s	192. ⊖ View URL Data	46467/TCP	-	Catch All	2.63K	SSH/SCP (unclassified)		
۲	Aug 10, 2017 9:17:40 AM	1m 43s	10 ⊡ View URL Data	50459/TCP	192.	Catch All	716	HTTP		
۲	Aug 10, 2017 9:16:40 AM	20s	10 ⊡ View URL Data	50459/TCP	192	Catch All	548	HTTP		
First	< 1 > Last									

サポートへの問い合わせ

テクニカル サポートが必要な場合は、次のいずれかを実行してください。

- 最寄りのシスコパートナーにご連絡ください。
- シスコサポートの連絡先
- Web でケースを開く場合:<u>http://www.cisco.com/c/en/us/support/index.html</u>
- 電子メールでケースを開く場合:<u>tac@cisco.com</u>
- 電話でサポートを受ける場合:800-553-2447(米国)
- ワールドワイドサポート番号: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

著作権情報

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標また は登録商標です。シスコの商標の一覧については、URL:<u>https://www.cisco.com/go/trademarks</u> をご覧ください。記載されている第三者機関の商標は、それぞれの所有者に帰属します。「パート ナー」という用語の使用はシスコ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。(1721R)