Firewalla ユーザマニュアル

ネットワークの防御① 見える化

ネットワークの防御① 見える化

家庭や中小企業をサイバー攻撃から保護するには、ネットワークデバイスのセキュリティを強化することが重要です。Firewallaはネットワーク全体を保護することで、すべてのIoTデバイスのセキュリティを強化します。

Firewallaは以下の機能によりネットワークのセキュリティを強化します。

- 1. 見える化 (Visibility): ネットワークを「見える化」します。ネットワークを完 全に把握し、リスクを特定できるようになります。
- 2. 制御(Control): ネットワークを制御し、重要なポリシーとルールを適用します。 これにより、攻撃対象領域が制限され、リスクが軽減されます。
- 3. 保護(Protect): Firewallaがルールに基づいてネットワークを自動的に保護します。



通信状況の見える化

Firewalla使用すると、自宅に接続されているデバイスの数やそれらのデバイスでどのような通信をおこなっているかを確認することができます。

ネットワークに接続されたデバイスの一部が、バックグラウンドで活発に動作している 状況などを確認することができます。

Firewallaは次のことに役立ちます。

- ネットワークに接続されたデバイスを把握する
- デバイスが何をしているかを確認する
- ネットワークを理解する
- 開いているポートを調べる
- アラームの確認と管理



ネットワークに接続されたデバイスを把握する

Firewallaをセットアップすると、家の中に接続されているすべてのデバイス (有線または無線) が表示されます。

すべての IoT デバイスの一覧が作成されます。それらが何であるかを確認し、Firewalla アプリで簡単に認識できるようにデバイスの名前を変更することができます。

ネットワーク上のデバイスには次のものが含まれる場合があります。

- スマートテレビ
- スピーカー
- プリンター
- カメラ
- 自動化制御ユニット など

Firewallaは、新しいデバイスが接続されるとアプリで通知します。また、オプションで、 新しいデバイスのネットワークアクセスを自動的に制限することもできます。たとえば、 隣人が許可なくあなたの Wi-Fi に接続した場合、すべてのインターネット アクセスをブ ロックすることができます。

ネットワークとグループでフィルタリングされたデバイスのリストを表示できます。 デバイス リスト全体をスクロールし、検索機能を使用して、名前、IP、またはMACアド レスでデバイスを見つけることもできます。



デバイスが何をしているか を確認する

Firewallaによりネットワーク内の各デバイスのトラフィックを確認することができます。 これは、特にバックグラウンドで動作するIoTデバイスに役立ちます。

ルーターは保護されたデータ接続の内容を確認できませんが、Firewallaは次のことを判断できます。

- ●データの送信先 (国、ドメインなど)
- どれくらいのデータが流れているのか
- ●どのようなトラフィック状況か
- ●インターネットへのアウトバウンド通信か、
- インターネットからのインバウンド通信か
- 許可されたかブロックされたか
- ●なぜ許可またはブロックされたのか

これらはデバイス、デバイス グループ、ネットワーク セグメントごとに確認できるため、 常に何が起こっているかを非常に明確かつ具体的に把握できます。 Firewallaは次のことを表示できます。

- 1. ネットワークフロー
- 2. ブロックされたフロー
- 3. ライブスループット

デバイスのアクティビティを定期的にチェックして、その動作を常に把握することができます。異常があればFirewallaによって自動的に検出され、アラートが届きます。



[Network Performanceの下部のFlows in Last24hrs] > [ネットワークのフロー]は、

ネットワーク上のすべての受信および送信ネットワーク トラフィックの履歴です。 [All Flows]内の取り消し線の項目は、ブロックされた内容を示します。

ブロックされたフローのみを表示する別のフィルターされたビューがあり、詳細が表示されます。

(詳細については、以下のブロックされたフローを参照してください)

11:19	all 🗢 🔳	11:20		all S	•
< Network	Flows	<	Network	Flows	
Last 24 Hours 👻	View Blocked	Last 24 Hours	~	Vie	w All
All Flows		Blocked Flows			
200,573		116,843	58.3% of	all flows	
Apps Upload	Download History	Top Block	ed	Blocked Flows	
Exclude Gaming S	Social Video Por	Exclude	Saming	Social Video	Por
11:19 AM 🛉 🔚 sandbox.itu	nes.apple.com	11:20 AM 🛉 🛄 📢	www.facebo	ok.com	IP
11:19 AM 🔹 📒 142.250.82.	12	11:19 AM • 🔤 t	reatment.gi	rammarly.com	DNS
11:19 AM 🔹 🎫 www.google	apis.com	11:17 AM 🛛 🔤 😆	stats.g.doub	leclick.net	DNS
11:19 AM 🛛 🗮 stun.l.googl	e.com	11:16 AM 🛛 🔤 🕇	metrics.iclo	ud.com	DNS
11:19 AM 🛛 🎬tension.fe	metrics.grammarly.io	11:16 AM • 📧 s	stats.g.doub	leclick.net	DNS
11:19 AM 🛛 📰 hangouts.go	ogleapis.com	11:14 AM • 🔤 t	reatment.gi	rammarly.com	DNS
11:19 AM 🛛 🎬 gateway.iclo	oud.com	11:14 AM 🛛 🏙 🕯	sl.gstatic.c	om	IP
11:19 AM 🛛 🎫 gateway.iclo	ud.com	11:13 AM 🛛 🔤 😆	stats.g.doub	leclick.net	DNS
11:19 AM 🛛 🗮 wss-primary	/.slack.com	11:13 AM 🛛 🚾 🤇	gnar.gramm	arly.com	DNS
11:19 AM 🛛 🎬 gateway.iclo	ud.com	11:12 AM • 🔤 s	stats.g.doub	leclick.net	DNS
11:19 AM 🛛 🗮 hangouts.go	ogleapis.com	11:10 AM 🖲 📧 t	reatment.gi	rammarly.com	DNS
11:19 AM 🛛 🏙 www.everno	te.com	11:10 AM • 🚾 s	stats.g.doub	leclick.net	DNS
11:19 AM 🛛 📰 adsmanager	r.facebook.com	11:09 AM 🖲 🚾	gnar.gramm	arly.com	DNS
11:19 AM 🛛 🚞 www.facebo	ok.com	11:07 AM 🖲 🚾 a	app-measur	ement.com	DNS
11:19 AM 🛛 🎬 adsmanager	r.facebook.com	11:06 AM 🖲 🔝 1	92.168.1.1		IP
11:19 AM 🛛 🔚 mtalk.googl	e.com	11:06 AM 🖲 🚾 🤇	gnar.gramm	arly.com	DNS
11:19 AM 🛛 🎬 imappro.zoh	io.com	11:04 AM • 🖾 t	reatment.g	rammarly.com	DNS
11:19 AM 🛛 🚍 www.google	apis.com	11:03 AM 🖲 🚾 🕯	stats.g.doub	leclick.net	DNS
11:19 AM 🔹 🧱 play.google.	com	11:02 AM • 🔤 a	app-measur	ement.com	DNS
11:19 AM 🖣 🚍 Hangoato.go	ogleapi s.com	11:02 AM 🛛 🔤	joogleada. g		DNS

このデータは、次のような内容を把握することができます。

- 1. デバイスはどのサーバーに接続しているか
- 2. これらのサーバーはどこにあるか
- 3. これらのサーバーには怪しい評判があるか
- 4. ブロックしたいデータ収集はあるか (ロギングやデータマイニングなど)
- 5. ポートのスキャンが行われていないか
- 6. どのような攻撃をうけているか

フローのリストを把握しやすくするために、除外(Exclude)機能を使用して一部のフローを ビューから非表示にすることができます。

- インバウンドフロー:外部から入ってくるフロー。通常、これらはブロックされます。
- ブロックされたフロー: Firewalla によって傍受されたフロー。
- システム ノイズ:システム ノイズを除外すると、OSシステム上のバックグラウンド トラ フィックと、よく見られるアプリ (広告、トラッキング、テレメトリ、ソフトウェア アッ プデート、分析、NTP、パブリック クラウド サービスを含む) がフィルタリングされます。

これは、ネットワーク内の重要なアクティビティに集中するのに役立ちます。 さらに、除外(Exclude)指定に特定のデバイスまたはターゲットを追加できます。 たとえば、特定の隔離されたデバイスからのブロックされたフローを表示したくない場合は、 そのデバイスを [ブロックされたフロー]に表示されないようにすることができます。

9:41	all 🗢 🛛	9:41		all 😤 🔳	9:41		all 🗢 🛛
K Netwood	ork Flows	<	Exclude		Cancel	Exclude Target	Don
Last 24 Hours 👻	View Blocked	EXCLUDE T	RAFFIC		e.g. drop		
All Flows		Inbound F	lows		Enter a targ	et to exclude from flows.	
284,230		Blocked F	lows		e.g.	10 1 2 2	
Apps Upload	Download History	System N	loise		Domain: go	ogle.com	
Exclude Gaming	Social Video Por	Excluding s important a	ystem noise helps you fo ctivity within your netwo	cus on rk.			
4:24 PM 🛛 🔚 s3-us-v	vest-2.amazonaws.com	EXCLUDE D	EVICE				
4:24 PM • 4:24 PM •		🕀 Add	Device				
4:24 PM • 4:24 PM • 📒ub-sh	ard2-19-4.zendesk.com	Loo Vide	eo Recorder				
4:24 PM • 1-1 3.ubunt	u.pool.ntp.org	L₀⊡ Can	nera 1				
4:24 PM • = 92.63.1	97.61 240.4	LoD Can	nera 2				
4:24 PM 🛛 🏪 host-ap	i.speedtest.net	EXCLUDE T	ARGET				
4:24 PM • 📒 www.sp 4:24 PM •	eedtest.net	🕀 Add	Target				
4:24 PM • Sagenter	nannel.api.duapp.com	IP 192	.168.2.67				
4:24 PM • = 185.222	2.222.222						
4:24 PM 🛛 🚾 1.1.1.2							
4:24 PM •	and the second sec						
4:24 PM 🛛 🎴 101.101.	101.101						
4:24 PM 🛛 🎦 1.1.1.1							

Webインターフェイスでは、地域ごとのトラフィックが表示されます。



Web インターフェイスでは、より複雑な分析のためにフィルタリングを行うこともできます。 この例では、「ブロック」は「ロシア」から流れてきます。

_									
	🜲 Firewalla - Netw	wrk Rows X +							
e ⇒ c	a my.firewalla	a.com(≢)hetwork?filters=b	locked-russia		¢ 🖬	🐂 🗄 🗖 🛛	1 5 🔍	- 🌣 📇 :	• 🚯
1							-	Gold F	_ → Sign Out
	Ddtd 11d	Insterreu						Last 24 Hour	5 *
88	↑ 1.6	GB Upload	55.7 GB Download	111,167 Flaws	31,230 B	locked Flaws		28.1% Block	ed
	8 GB								
Δ	7.08 ···		\wedge						
- T	5 GB			\frown					
Ga	4 GB		$\gamma \mid \gamma \mid$	- 10	\wedge			~	
COU	2 GB		$ \rightarrow / / / / / / / / / / / / / / / / / / $	·····		~	\sim	$ \land $	
	1 GB		\mathbf{V}			~		1	
\diamond	9 AM	12 PM	6 PM		12 AM		6 AM	9.A	M
~	-								
V	a a	blocked × Q rus	sia ×		Clear All	Last	24 Hours		~)
							< 1	$2 \rightarrow 200/p$	age 🗸
	Timestamp	Source	Destination	Destination Port	Network	Category	Status	Blocked By	
	9:25 AM	92.63.197.12	🥥 Sall Internet	TCP 63734	Sall Internet	-	 Blocked 	IP Filtering	
\approx	9:25 AM	92.63.197.12	🥥 Sall Internet	TCP 17460	🗞 Sall Internet	-	 Blacked 	IP Filtering	
	9:24 AM	92.63.197.12	🥥 Sall Internet	TCP 43500	🔁 Sall Internet		 Blocked 	IP Filtering	
	9:24 AM	45.146.166.121	🥥 Sall Internet	TCP 54894	Sall Internet	-	 Blocked 	IP Filtering	
	9:24 AM	92.63.197.12	🥥 Sall Internet	TCP 45677	😚 Sall Internet	-	 Blacked 	IP Filtering	
0	9:24 AM	92.63.197.12	🥥 Sall Internet	TCP 38804	🔁 Sall Internet	-	 Blacked 	IP Filtering	
v1465	9:24 AM	92.63.197.12	🥥 Sall Internet	TCP 44626	😓 Sall Internet	-	 Blocked 	IP Filtering	
Cond V	9-23 AM	92 63 197 12	C Sall Internet	TCP 9242	Sall Internet		 Blackert 	IP Filtering	

2. ブロックされたフロー

ブロックされたフローでは、Firewallaによってブロックされた通信を確認できます。例えば、 広告ブロックが期待どおりに機能しているかどうかを知ることができます。これらは、設定し たルールを微調整したり、アクセスを許可またはブロックする新しいルールを作成したりする のに役立ちます。

ブロックフローの右の列をタップすると、以下の表示データを順番に切り替えることができます。

- 1. ブロック数:特定のドメインまたはIPが何回ブロックされたか
- 2. インバウンドとアウトバウンド:ネットワークの外から入った通信か、それともネット ワークの内部から外への通信か
- 3. ブロックの理由: Firewallaが接続をブロックしたのはなぜか
- 4. ポート: どのポート番号がアクセスされていたか



また、ブロックされたフローのエントリのいずれかをクリックすると、トラフィックの 発信元または宛先であるサーバーの場所、使用された WAN 接続、使用されたポート、 およびブロックされた理由の詳細を確認することもできます。

特定のIPアドレスまたはドメインについてさらに詳しく調べることもできます。 これにより、そのサーバーに接続するリスクを確認することができます。



- Firewallaは、地域と宛先ごとにブロックされた上位フローの2つのリストを表示します。
- トップリージョン+インバウンド: 外部からの誰かがネットワークに接続しようとすると、
 ほとんどの接続はFirewallaのIngress Firewallによってブロックされます。
 これらのフローを地域に基づいて集計します。
- 上位の宛先 + 送信:これらは、デバイスが接続しようとしている宛先です。



ライブ スループットはアップロードとダウンロードのアクティビティをリアルタイムで 測定します。

注: iOSを使用している場合は、Firewallaアプリがローカル ネットワークにアクセスで きることを確認してください。

[設定] で、**[プライバシー] > [ローカル ネットワーク]**に移動し、Firewallaアプリへの アクセスを許可します。 ライブ スループットは個々のデバイス単位で確認できます。





さらに、1.53 アプリ リリースの一部として、ローカル ネットワークに接続している間、 デバイス リストに個々のライブ スループットが表示されるようになりました。 ビデオ チュートリアルを参照するか、 Firewallaアプリ リリース 1.53 ノートでこの機 能の詳細を参照してください。



ネットワークを理解する

Firewallaには、ネットワークパフォーマンスの監視と向上に役立つツールが用意されています。

Firewallaは、LAN/Wi-FiネットワークとWANの両方でインターネット速度、ネットワーク遅延、ネットワークパケット損失を測定できます。

Firewallaは、Wi-Fi接続をリアルタイムでテストおよび調整するのに役立つWi-Fiテスト機能も提供します。

この機能を使用するには、ボックスのローカルWi-Fiに接続していることを確認し、[Wi-Fiテスト]をタップします。

接続のダウンロード速度、アップロード速度、ping遅延、Wi-Fiローミングに関する情報 を確認できます。

Firewallaでは、過去30日、24時間、および60分間のアップロードおよびダウンロードの合計データ消費量を表示できます。

これにより、月の中で最も活動的な日、1日の時間、または1時間の分を観察できます。 これは、異常なアクティビティを見つけたり、ネットワークのボトルネックを特定したり するのに役立ちます。

^		.
	Gold Managed	铰
Flows in last 24 hours 116,140	Blocked 35,314	30.4%
150GB	La	st 30 Days
120GB		٨
90GB		/ \
60GB		
30GB	\frown	
•		$\smile \kappa$
0B Oct 12, 2021 Oct 21, 2021 • 38.77 GB Upload • 1.04	Oct 31, 2021 4 TB Download 1	Nov 10, 2021
0B Oct 12, 2021 Oct 21, 2021 • 38.77 GB Upload • 1.04	4 TB Download 1 Internet	Nov 10, 2021
0B Oct 12, 2021 Oct 21, 2021 • 38.77 GB Upload • 1.04 Live Throughput - Sall	4 TB Download 1 Internet	Nov 10, 2021
08 Oct 12, 2021 Oct 21, 2021	0 oct 31, 2021 4 TB Download 1 Internet ↓ 45.8 MI	Nov 10, 2021 1.08 TB Total
08 Oct 12, 2021 Oct 21, 2021 • 38.77 GB Upload • 1.04 ■ Live Throughput - Sall ↑ 543 kb/s Upload Live Throughput - LTE	4 TB Download 1 Internet	Nov 10, 2021 1.08 TB Total
08 Oct 12, 2021 Oct 21, 2021	A TB Download 1 Internet	Nov 10, 2021 1.08 TB Total
08 Oct 12, 2021 Oct 21, 2021	Oct 31, 2021 TB Download 1 Internet ↓ 45.8 MI 45.8 MI 45.8 MI	Nov 10, 2021 1.08 TB Total
Oct 12, 2021 Oct 21, 2021	 Oct 31, 2021 4 TB Download 1 Internet 45.8 MI 45.8 MI 	Nov 10, 2021 1.08 TB Total D/S Download S Download

過去のデータ使用量を調べたい場合は、ボックスのメインページの一番下までスクローし、 [**詳細] > [データ使用量]**機能をタップします。

この機能では、月ごとのデータ使用量グラフと日ごとのデータ使用量グラフが表示されます。 各グラフをタップすると詳細が表示され、月間のデータ消費量を比較できます。

インターネット接続にデータ制限がある場合、Firewallaは消費したデータ量と請求サイクルの残り日数を監視できます。

また、ISPからのペナルティを避けるために、データの上限に達しそうになったときに通知するアラームを設定することもできます。

≻	14:12	۰ 🕱 96% 🖲	₽	VPN	14:13	
<	Alarms	日式	<			
Q Search			ता Mar	Monthly 26, 2020 at 1	Data Plan 4:03	
Monthly Da Mar 26, 2020 at 14:03	a ta Plan 3		The 148	monthly d 16% of the	data usage has i e plan. (148.16 (reached GB of 100 GB)
The monthly data	a usage has re	ached	DAT	A USAGE		
148.16% of the p	lan. (148.16 GI	3 of 100 GB)	14	8.16 GB	used 48.1	16 GB exceede
	Archive		6 da	ays left in t	his cycle	
E	Earlier Alarms –		DAT/		RED	
C Large Band Mar 26, 2020 at 13:04	lwidth Usage		25GB			
Device Annies-M the past 2 hours	lac consumed (98.97% of tot	3.13 GB in al).	20GB 15GB 10GB		٨	
🕅 Mute	(Block	5GB 0B	lar-01		21 Apr-01
VPN Activit Mar 26, 2020 at 12:04	y 4			• 19 GB Uploa	ad • 129 GB Downloa	ad 148 GB Total
IP 49.76.55.32 co	onnected to Fi	rewalla VPN.			T Archive	
					_	

[ネットワーク フロー]の[アプリ]ビューを使用すると、ネットワーク、グループ、または デバイスがアプリ/ドメインごとに費やしているおおよその時間を確認できます。アップ ロードとダウンロードを使用して、データ使用量の上位を確認してください。

.ul 🗢 🔳 9:41 10:52 ୶ ...| 🌫 🚱 Network Flows Network Flows < Today, 12:00 PM - 1:00 PM - View Blocked Last 24 Hours 👻 All Flows 284,230 All Flows View Blocked 112,966 Upload Download History Apps Upload Download History TOP DEVICES Apps 13.02 GB 1 Server YOUTUBE (373 MIN) 2 J MyiPhone 11.25 GB 07:00 AM • 32 seconds 04:58 AM • 8 min 3 🚺 My Macbook 8.84 GB 04:49 AM 🛉 7 min 04:38 AM 🛉 2 min 4 In Android 5.12 GB 04:27 AM • 8 min 5 🚮 Bedroom 1.52 GB 04:20 AM 🛉 2 min 02:45 AM • 60 seconds Show All 02:29 AM • 27 seconds TOP DESTINATIONS 01:22 AM 🛉 60 min 11:28 PM 🛉 3 min 1 📒 googleapi.com 6.57 GB 11:17 PM • 9 min 2 measurement-lab.org 3.17 GB 11:06 PM 🛉 6 min 10:57 PM • 9 min 3 📁 googlevideo.com 1.74 GB 10:47 PM 🛉 8 min 4 📒 yahoo.com 1.60 GB 10:17 PM 🛉 25 min 09:09 PM 🛉 60 min 5 📒 nfxvideo.net 1.47 GB > 07:28 PM • 17 min Show All 06:37 PM • 8 min 06:16 PM • 20 min TOP FLOWS 05:42 PM • 115 seconds

Webインターフェイスには、アップロードとダウンロードの上位デバイスと宛先が表示されます。

op Devices by Opioad			Last 2-4 Hours	Top Devices by Downlo	30	Last 24 m
Device	Uploa	ad	Download	Device	Upload	Download
📃 BigMac Ethernet 💻	554.5	5 MB	5 GB	Apple TV: Living Room	943.2 MB	21 GB
🐵 Michael's MacBook Pro	377.9	9 MB	6 GB	🗔 Apple TV: Kitchen 📃	22.6 MB	9.1 GB
💶 Security Cameras 🞇	301.4	4 MB	250.4 KB	🛄 Michael's iPad 🚞	44.1 MB	7.3 GB
📮 Jovana's iPad 📃	60.41	MB	1.2 GB	Michael's MacBook Pro	377.9 ME	6 GB
Michael's iPad	44.11	MB	7.3 GB	BigMac Ethernet	554.5 M	5 GB
op Destinations by Uple	load		Last 24 Hours	Top Destinations by Do	wnload	Last 24 Ho
op Destinations by Uple	load	THE	Last 24 Hours	Top Destinations by Do	wnload Region	Last 24 Ho Download
Top Destinations by Uple	load Region Suited States	HD .	Last 24 Hours Upload 599.4 MB	Top Destinations by Do Destination	wnload Region States	Last 24 Ho Download 25.4 GB
op Destinations by Uple Destination 173.46.67.114	load Region United States		Last 24 Hours Upload 599.4 MB 471.5 MB	Top Destinations by Do Destination dssott.com googlevideo.com	wnload Region United States	Last 24 Ho Download 25.4 GB 9.8 GB
For Destinations by Uple Destination 173.46.67.114 Zoom.us ooklaserver.net	load Region United States United States United States		Last 24 Hours Upload 599.4 MB 471.5 MB 173.4 MB	Top Destinations by Do Destination dssott.com googlevideo.com cdn-apple.com	wnload Region United States United States United States	Last 24 Ho Download 25.4 GB 9.8 GB 6.3 GB
Fop Destinations by Uple Destination 173.46.67.114 Zoom.us ooklaserver.net google.com	load Region United States United States United States United States		Last 24 Hours Upload 599.4 MB 471.5 MB 173.4 MB 48.7 MB	Top Destinations by Do Destination dssott.com googlevideo.com cdn-apple.com apple.com	wnload Region United States United States United States United States	Last 24 Ho Download 25.4 GB 9.8 GB 6.3 GB 3.9 GB

開いているポートを調べる

Firewallaは、次の開いているポートを検出できます。

- 外部スキャンされたポート:外部スキャンによって検出されたポート。
- UPnP ポート: UPnPプロトコルを使用して検出されたポート。これらのポートは、 UPnP経由で他のデバイス/サービスによって開かれます。

「ポートを開く」ボタンをタップすると、これらのポートが表示されます。 それぞれのポートが開いている理由を必ず理解してください。 ルーターでポートを開く必要がある場合は、Firewalla VPNサーバーを使用してそのデバ イスにアクセスする方が良い解決策と考えられます。

アラームの確認と管理

Firewallaは、不審なアクティビティが発生した場合にアラームと通知で警告します。 アラートには次のようなものが含まれます。

- 1. ポルノ活動
- 2. ゲーム活動
- 3. 警備活動
- 4. WAN接続の問題

(Wi-Fiに問題があるのか、ISPがダウンしているのかを推測する必要はありません)

- 5. VPN接続と接続の喪失
- 6. デバイスがオン/オフラインになる
- 7. ネットワーク イベント、ISPダウンタイム、および接続テストの結果
- 8. 大量の帯域幅の使用量
- 9. 新しいデバイスの接続
- 10.ポートを開く

これらのアラートは、ネットワークを管理するのに役立ちます。

アラームが通常の操作または信頼できるサービスに関連付けられている場合は、アラーム を無視またはミュートできます。

ただし、デバイスのアクティビティが予期しないものである場合は、調査するかブロック する必要があります。

6:28 Search			•
<			
🙆 Large Bandy	width Usaq		
Jun 14, 2020 at 10:20	PM		
Device Smart TV i GB in the past 2 h	n living roon ours (92.549	n consumed 2.7 % of total).	2
DEVICE			
Name	Sma	rt TV in living r	oon
IP Address		10.0.1	.11:
MAC Address			
Vendor	Но	n Hai Precision	Ind
Network			
DATA TRANSFERRED			
Data transferred	in the last 2	4 hours.	
1208			
108			
BDDMB			
600MB			
400MB			
200MB			1
08			П
10:30 PM 06	(15 AM	02/15 PM 1	
 4.3 MB Uploa 	a • 2.7 GB Dow	nioad 2.7 GB Total	

Webインターフェイスを使用すると、アラーム検索をフィルタリングできます。 たとえば、ハートビート攻撃のセキュリティ アクティビティは次のようになります。

Q Security Activity × Q heartbeat ×			금는 Alarm Settings	
Export	ö	Security Activity		11/1/2021 10:56 PM
Security Activity 11/1/2021 10:56 PM Heartbeat message smaller than minimum required length. Probable attack. Message length: 27. Required length: 43. Cipher: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256. Cipher match: /^?(_AES_128_GCM_SHA256\$)\$?/		Heartbeat message sm. Message length: 27. Re TLS_ECDHE_RSA_WIT (AES_128_GCM_SHA2 Transformer and the second	aller than minimum required length. I quired length: 43. Cipher: H_AES_128_GCM_SHA256. Cipher n :56\$)\$?/ Delete	Probable attack. natch: /^?
		Device		
		Name	Pigpen / Synology NAS 📳	
		MAC Address	8118.00.010	
		IP Address	192.168.0.19	
		Vendor	Synology Incorporated	
		Status	• Online	
		Network	LAN 0	