

Deployment Guide

GIGA スクール構想対応ネットワークソリューション

学校からの広帯域通信のブレイクアウト (SD-WAN) 設定ガイド

- NHK for School ビデオコンテンツ
- YouTube
- ビデオ会議システム (Zoom)

免責事項

本ドキュメントに関する著作権は、フォーティネットジャパン株式会社へ帰属します。フォーティネットジャパン株式会社が事前に承諾している場合を除き、形態及び手段を問わず本ドキュメントまたはその一部を複製する事は禁じられています。

また本内容は参考例となります。個別のセキュリティ対策に関する要件を満たすには、ご利用者様ごとにプランニングおよび設定の調整が必要となりますので、予めご了承下さい。尚、本ドキュメントの作成にあたっては最新の注意を払っておりますが、その記述内容は予告なしに変更される事があります。

目次

1. はじめに.....	5
1.1. 利用機器と OS バージョン	5
1.2. 構成.....	5
1.3. 参照資料.....	6
2. インターネットブレイクアウト対象通信.....	7
1.1. NHK for School	7
1.2. YouTube.....	7
1.3. ビデオ会議システム (Zoom)	7
3. NHK for School ドメインの登録	8
3.1. nhks-vh.akamaihd.net の設定	9
3.2. nhk-vh.akamaihd.net の設定.....	10
3.3. 確認.....	11
4. SD-WAN ルールによるインターネットブレイクアウト.....	12
4.1. SD-WAN インターフェースの設定	12
4.2. NHK for School の SD-WAN ルールの設定.....	15
4.3. Zoom、YouTube の SD-WAN ルールの設定	17
4.4. 通常トラフィックの SD-WAN ルールの設定.....	19
4.5. SD-WAN インターフェース向けスタティックルートの設定	21
4.6. IPv4 ポリシーの設定	22
4.7. 動作確認.....	24
5. Appendix: スタティックルートによるインターネットブレイクアウト	25
5.1. スタティックルートの設定	25

5.2. IPv4 ポリシーの設定	26
5.3. 動作確認	26

1.はじめに

この設定ガイドは、GIGA スクール構想において利用が想定されている広帯域通信(NHK for School・YouTube・ビデオ会議システム)を、インターネットブレイクアウトする方法について解説します。

インターネットブレイクアウトとは複数の WAN 回線を用意し、特定のトラフィックの通信経路を制御（例：特定のトラフィックのみ安価な WAN 回線を利用する、など）して、拠点から直接インターネットへ通信させる機能です。クラウドアプリケーションの利用による、ネットワークリソースのひっ迫を FortiGate の機能を用いて低減させることが目的で利用されます。本ガイドでも2つの WAN 回線が存在することを前提にしています。

1.1. 利用機器と OS/ソフトウェアバージョン

FortiGate	FortiGate-VM	Version 6.2.3
FortiGate	ISDB	Version 7.00702

1.2. 構成

物理構成

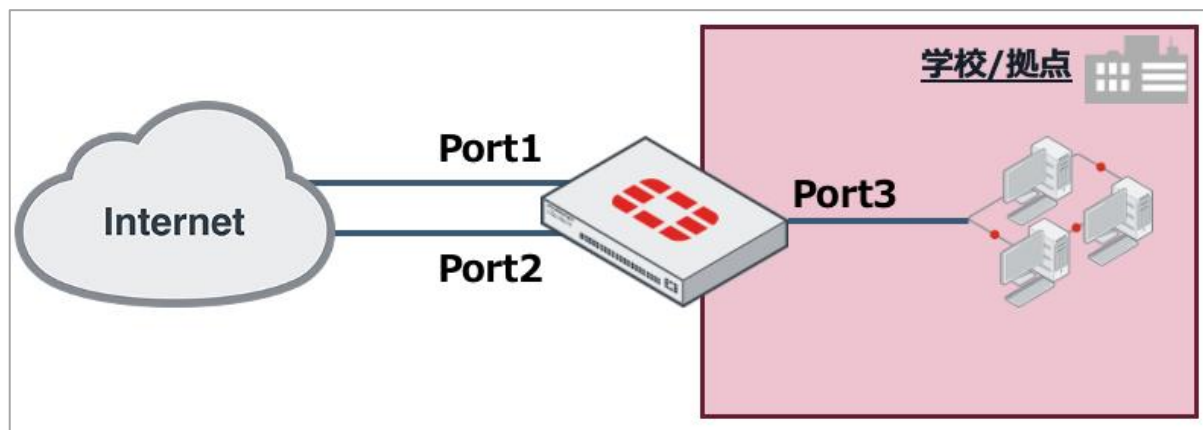


図 1-1 物理構成図

論理構成

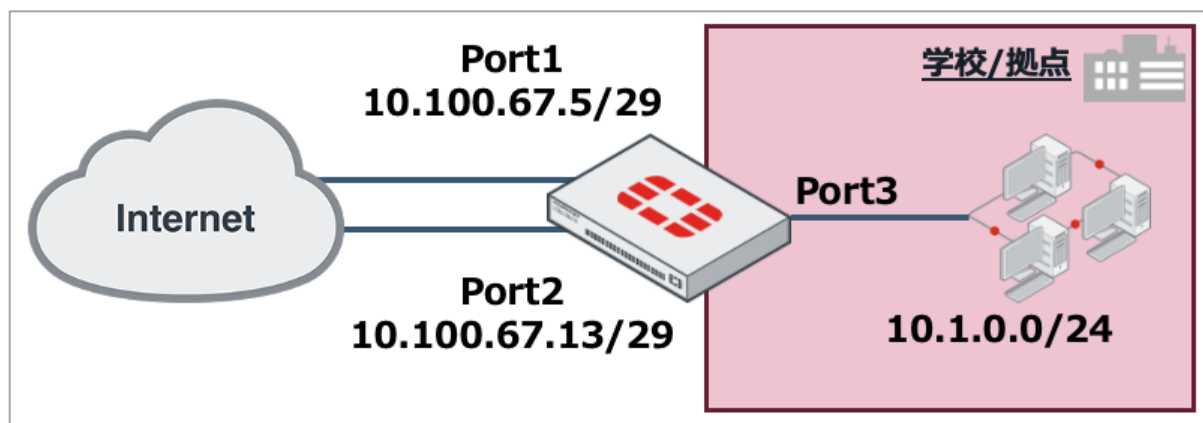


図 1-2 論理構成図

インターネットブレイクアウト構成

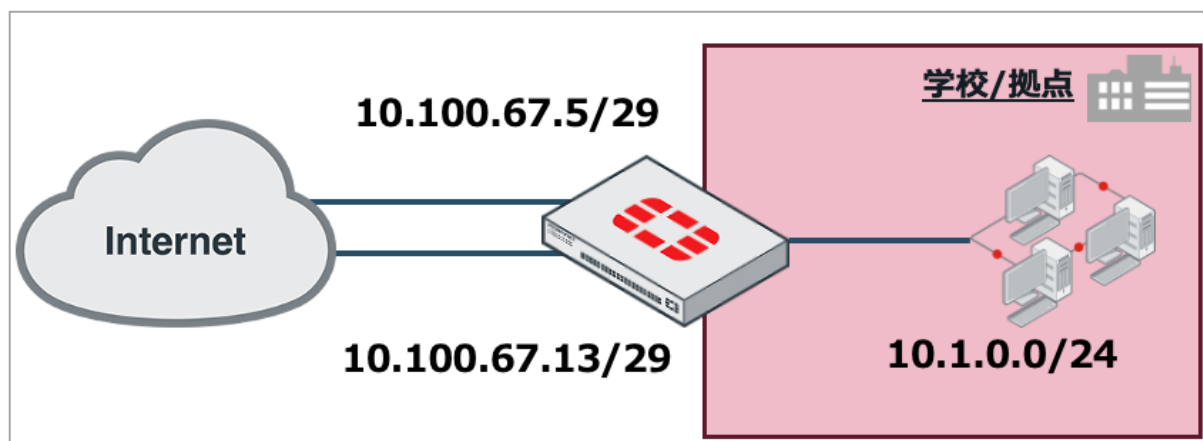


図 1-3 インターネットブレイクアウト構成図

1.3. 参照資料

本設定ガイドで紹介している設定は公式な設定ガイドに基づいています。より詳細な情報が必要な場合は以下も合わせてご参照ください。

FortiGate / FortiOS 6.2.3 Cookbook SD-WAN

<https://docs.fortinet.com/document/fortigate/6.2.3/cookbook/19246/sd-wan>

2. インターネットブレイクアウト対象通信

本設定ガイドでは、GIGA スクール構想で使用される可能性が高い3つのトラフィックをインターネットブレイクアウトの対象とします。

1.1. NHK for School

NHK が提供する、学校放送番組やウェブサイトなど学校向けサービス。

1.2. YouTube

Google が提供する世界最大の動画共有サービス。

1.3. ビデオ会議システム (Zoom)

遠隔授業を実施するためのリアルタイムメッセージングとコンテンツ共有が可能なビデオ会議システム。

* 本ガイドでは代表例として Zoom の設定方法を記載します。

3.NHK for School ドメインの登録

NHK for School は FortiGate の ISDB（インターネットサービスデータベース：インターネット上のサービスと IP アドレス、ポート情報を紐付けた Fortinet 独自のデータベース）に登録されていないため、手動でアドレスオブジェクトを作成します。NHK for School のビデオコンテンツは以下をソースとしています。

nhks-vh.akamaihd.net

nhk-vh.akamaihd.net

この二つの FQDN を登録し、アドレスリストやスタティックルートに表示されるように設定します。

* 上記は 2020/4/1 時点の情報をもとに作成しています。

3.1. nhks-vh.akamaihd.net の設定

左メニュー「ポリシー&オブジェクト」→「アドレス」をクリックし、「新規作成」→「アドレス」をクリックし、ドメイン情報を入力します。

名前 : NHK1

カラー : 任意

タイプ : FQDN

FQDN : nhks-vh.akamaihd.net

インターフェース : any

Show in address list : 有効

Static route configuration : 有効

コメント : 任意

The screenshot shows the FortiGate configuration interface. On the left, the 'Policy & Object' menu is expanded to 'Addresses'. The main area displays the 'New Address' configuration form. The fields are as follows:

- 名前: NHK1
- カラー: 変更
- タイプ: FQDN
- FQDN: nhks-vh.akamaihd.net
- インターフェース: any
- Show in address list:
- Static route configuration:
- コメント: コメント記入 (0/255)

図 3-1 nhks-vh.akamaihd.net 設定

3.2. nhk-vh.akamaihd.net の設定

左メニュー「ポリシー&オブジェクト」→「アドレス」をクリックし、「新規作成」→「アドレス」をクリックし、ドメイン情報を入力します。

名前 : NHK2

カラー : 任意

タイプ : FQDN

FQDN : nhk-vh.akamaihd.net

インターフェース : any

Show in address list : 有効

Static route configuration : 有効

コメント : 任意

The screenshot shows the FortiGate web interface for configuring a new address object. The left sidebar contains a navigation menu with 'アドレス' (Addresses) selected. The main panel is titled '新規アドレス' (New Address) and contains the following fields:

- 名前 (Name): NHK2
- カラー (Color): [Change icon]
- タイプ (Type): FQDN
- FQDN: nhk-vh.akamaihd.net
- インターフェース (Interface): any
- Show in address list:
- Static route configuration:
- コメント (Comment): コメント記入 (0/255)

図 3-2 nhk-vh.akamaihd.net 設定

3.3. 確認

左メニュー「ポリシー&オブジェクト」→「アドレス」をクリックします。作成したアドレスにマウスオーバーすることで FQDN から引いた IP アドレスを確認可能です。

* 正引きされる IP アドレスは環境やタイミングにより変わる可能性があります。GUI に表示されている IP アドレスは一例であり、必ずしも同一の IP アドレスになるわけではありません。

名前	タイプ	詳細
FABRIC_DEVICE	サブネット	0.0.0.0/0
FIREWALL_AUTH_PORTAL_ADDRESS	サブネット	0.0.0.0/0
Finance Network	サブネット	10.100.92.0/24
HQ_ISFW	サブネット	10.100.88.0/24
HQ_Server_Farm	サブネット	10.100.77.0/24
HQ_VPN_Gwy_A	サブネット	10.100.64.101/32
HQ_VPN_Gwy_B	サブネット	10.100.65.101/32
IT Network	サブネット	10.100.93.0/24
Marketing Network	サブネット	10.100.91.0/24
NHK1	FQDN	nhks-vh.akamaihd.net
NHK2	FQDN	nhk-vh.akamaihd.net

nhks-vh.akamaihd.net 解決先:

- 23.35.111.27
- 23.35.111.34
- 23.62.109.94
- 23.62.109.111

図 3-3 nhks-vh.akamaihd.net の IP アドレス確認

名前	タイプ	詳細
Finance Network	サブネット	10.100.92.0/24
HQ_ISFW	サブネット	10.100.88.0/24
HQ_Server_Farm	サブネット	10.100.77.0/24
HQ_VPN_Gwy_A	サブネット	10.100.64.101/32
HQ_VPN_Gwy_B	サブネット	10.100.65.101/32
IT Network	サブネット	
Marketing Network	サブネット	
NHK1	FQDN	
NHK2	FQDN	

nhk-vh.akamaihd.net 解決先:

- 23.56.170.40
- 23.32.3.64

図 3-4 nhk-vh.akamaihd.net の IP アドレス確認

4. SD-WAN ルールによるインターネットブレイクアウト

4.1. SD-WAN インターフェースの設定

左メニュー「ネットワーク」→「SD-WAN」をクリックし、「有効」をクリックします。

ダッシュボード	>	SD-WAN
セキュリティアプリケーション	>	名前 SD-WAN
FortiView	>	タイプ SD-WANインターフェース
ネットワーク	>	ステータス 有効 無効
インターフェース		SD-WANインターフェースメンバー
DNS		+ 新規作成 編集 削除
パケットキャプチャ		インターフェース ゲートウェイ コスト
SD-WAN	☆	エントリがありません
SD-WANルール		
パフォーマンスSLA		
スタティックルート		

図 4-1 SD-WAN 設定

次に「新規作成」をクリックし、SD-WAN インターフェースメンバーの設定を行います。

インターフェース : port1

ゲートウェイ : 0.0.0.0

* 動的にデフォルトゲートウェイを取得する場合は 0.0.0.0 を設定します。

コスト : 任意 (例. 0)

ステータス : 有効

The screenshot shows the 'Edit SD-WAN Member' configuration page. The interface is divided into several sections. The 'インターフェース' (Interface) section has a dropdown menu with 'port1' selected. The 'ゲートウェイ' (Gateway) section has a dropdown menu with 'ダイナミック' (Dynamic) selected and a '指定' (Specify) button, followed by a text input field containing '0.0.0.0'. The 'コスト' (Cost) section has a text input field containing '0'. The 'ステータス' (Status) section has two radio buttons: '有効' (Enabled) which is selected, and '無効' (Disabled). A red rectangular box highlights the 'port1', '0.0.0.0', and '有効' fields.

図 4-2 SD-WAN 設定 (port1)

続いて、2つ目のインターフェースの設定を行います。

インターフェース : port2

ゲートウェイ : 0.0.0.0

* 動的にデフォルトゲートウェイを取得する場合は 0.0.0.0 を設定します。

コスト : 任意 (例. 0)

ステータス : 有効

The screenshot shows the 'Edit SD-WAN Member' configuration page. The settings are as follows:

インターフェース	port2
ゲートウェイ	ダイナミック 指定 0.0.0.0
コスト	0
ステータス	有効 無効

図 4-3 SD-WAN 設定 (port2)

2つのインターフェースを登録できたことを確認し、「適用」をクリックします。

4.2. NHK for School の SD-WAN ルールの設定

左メニュー「ネットワーク」→「SD-WAN ルール」をクリックし、「新規作成」をクリックします。

名前 : GIGA_School_NHK

送信元アドレス : all

ユーザグループ : 選択しない

アドレス : NHK1, NHK2

プロトコル番号 : ANY

インターネットサービス : 選択しない

アプリケーション : 選択しない

ストラテジー : マニュアル

→基本的に優先するインターフェースでのみ通信を行います。優先するインターフェースがダウンした場合は、他の SD-WAN インターフェースで通信を行います。

優先するインターフェース : port2

ステータス : 有効

ダッシュボード	>	プライオリティルール
セキュリティファブリック	>	
FortiView	>	
ネットワーク	▼	
インターフェース		
DNS		
パケットキャプチャ		
SD-WAN		
SD-WANルール	☆	
パフォーマンスSLA		
スタティックルート		
ポリシールート		
RIP		
OSPF		
BGP		
マルチキャスト		
システム	>	
ポリシー&オブジェクト	>	
セキュリティプロファイル	>	
VPN	>	
ユーザ&デバイス	>	

名前	GIGA_School_NHK
送信元	
送信元アドレス	all
ユーザグループ	
宛先	
アドレス	NHK1 NHK2
プロトコル番号	TCP UDP ANY 指定する 0
インターネットサービス	
アプリケーション	
発信インターフェース	
ストラテジー	マニュアル ベストクオリティ 最小コスト(SLA) 帯域幅の最大化(SLA)
優先するインターフェース	port2
ステータス	有効 無効

図 4-4 SD-WAN ルール設定 (NHK for School)

4.3. Zoom、YouTube の SD-WAN ルールの設定

左メニュー「ネットワーク」→「SD-WAN ルール」をクリックし、「新規作成」をクリックします。

名前 : GIGA_School_Zoom_YouTube

送信元アドレス : all

ユーザグループ : 選択しない

アドレス : 選択しない

インターネットサービス : "Zoom.us-Zoom.Meeting"

→Zoom の他のサービスもブレイクアウトしたい場合は、該当サービスを選択します。

* ISDB のバージョンによっては、インターネットサービスで指定するオブジェクトが変更になる場合があります。本設定ガイドでは ISDB Version 7.00702 を利用しているため"Zoom.us-Zoom.Meeting"を指定します。

アプリケーション : "YouTube"

→YouTube の全ての通信をブレイクアウトさせる場合は"YouTube"を選択します。

ストラテジー : マニュアル

→基本的に優先するインターフェースでのみ通信を行います。優先するインターフェースがダウンした場合は、他の SD-WAN インターフェースで通信を行います。

優先するインターフェース : port2

ステータス : 有効

4.4. 通常トラフィックの SD-WAN ルールの設定

左メニュー「ネットワーク」→「SD-WAN ルール」をクリックし、「新規作成」をクリックします。

名前 : All

送信元アドレス : all

ユーザグループ : 選択しない

アドレス : all

インターネットサービス : 選択しない

アプリケーション : 選択しない

ストラテジー : マニュアル

→基本的に優先するインターフェースでのみ通信を行います。優先するインターフェースがダウンした場合は、他の SD-WAN インターフェースで通信を行います。

優先するインターフェース : port1

ステータス : 有効

<ul style="list-style-type: none"> ダッシュボード > セキュリティファブリック > FortiView > ネットワーク > インターフェース DNS パケットキャプチャ SD-WAN SD-WANルール ☆ パフォーマンスSLA スタティックルート ポリシールート RIP OSPF BGP マルチキャスト システム > ポリシー & オブジェクト > セキュリティプロファイル > VPN > ユーザ & デバイス > 	<p>プライオリティルール</p> <p>名前 <input type="text" value="All"/></p> <p>送信元</p> <p>送信元アドレス <input style="border: 1px solid #ccc;" type="text" value="all"/> ✕</p> <p style="text-align: center;">+</p> <p>ユーザグループ <input style="border: 1px solid #ccc;" type="text" value=""/> +</p> <p>宛先</p> <p>アドレス <input style="border: 1px solid #ccc;" type="text" value="all"/> ✕</p> <p style="text-align: center;">+</p> <p>プロトコル番号 TCP UDP ANY 指定する <input style="width: 30px;" type="text" value="0"/></p> <p>インターネットサービス ⓘ <input style="border: 1px solid #ccc;" type="text" value=""/> +</p> <p>アプリケーション ⓘ <input style="border: 1px solid #ccc;" type="text" value=""/> +</p> <p>発信インターフェース</p> <p>ストラテジー マニュアル</p> <p style="margin-left: 20px;"> ベストクオリティ 最小コスト(SLA) 帯域幅の最大化(SLA) </p> <p>優先するインターフェース <input style="border: 1px solid #ccc;" type="text" value="port1"/> ▼</p> <p>ステータス 有効 無効</p>
---	--

図 4-6 SD-WAN 設定 (通常トラフィック)

4.5. SD-WAN インターフェース向けスタティックルートの設定

左メニュー「ネットワーク」→「スタティックルート」をクリックし、「新規作成」をクリックします。

ダイナミックゲートウェイ：無効

宛先：サブネット → 0.0.0.0/0.0.0.0

インターフェース：SD-WAN

アドミニストレーティブ・ディスタンス：10

* 10を設定すると、SD-WAN インターフェースではアドミニストレーティブ・ディスタンス値は1が設定されます。

コメント：任意

ステータス：有効化済み

The screenshot shows the 'New Static Route' configuration page in the FortiGate web interface. The left sidebar shows the navigation menu with 'Network' expanded and 'Static Route' selected. The main content area shows the configuration for a new static route. The 'Dynamic Gateway' toggle is turned off. The 'Destination' is set to 'Subnet' with the value '0.0.0.0/0.0.0.0'. The 'Interface' is set to 'SD-WAN'. The 'Administrative Distance' is set to '10'. The 'Comment' field is empty. The 'Status' is set to 'Activated'. An 'OK' button is visible at the bottom right.

図 4-7 SD-WAN インターフェース向けスタティックルート設定

4.6. IPv4 ポリシーの設定

左メニュー「ポリシー&オブジェクト」→「IPv4 ポリシー」をクリックし、「新規作成」をクリックします。

名前 : GIGA_School

着信インターフェース : port3

発信インターフェース : SD-WAN

送信元 : all

宛先 : all

スケジュール : always

サービス : ALL

アクション ACCEPT

インスペクションモード : 任意 (例. フローベース)

NAT : 任意 (例. 有効)

IP プール設定 : 任意 (例. 発信インターフェースのアドレスを使用)

送信元ポートの保持 : 任意 (例. 無効)

プロトコルオプション : default

アンチウイルス : 任意 (例. 無効)

Web フィルタ : 任意 (例. 無効)

DNS フィルタ : 任意 (例. 無効)

アプリケーションコントロール : 有効 → default

→デフォルトのプロファイルは全アプリケーションがモニタの設定です。YouTube アプリケーションを検出する必要があるため、ここではデフォルトプロファイルを使用します。

IPS : 任意 (例. 無効)

SSL インスペクション : certificate-inspection

許可トラフィックをログ : 任意 (例、有効 → すべてのセッション)

セッション開始時にログを生成 : 任意 (例、無効)

パケットをキャプチャ : 任意 (例、無効)

このポリシーを有効化 : 有効

Edit Policy

名前 **GIGA_School**

着信インターフェース **port3**

発信インターフェース **SD-WAN**

送信元
all

宛先
all

スケジュール **always**

サービス **ALL**

アクション **ACCEPT** DENY

インスペクションモード **フローベース** プロキシベース

ファイアウォール/ネットワークオプション

NAT

IPプール設定 **発信インターフェースのアドレスを使用** ダイナミックIPプールを使う

送信元ポートの保持

プロトコルオプション **PRX default**

セキュリティプロファイル

アンチウイルス

Webフィルタ

DNSフィルタ

アプリケーションコントロール **APP default**

IPS

SSLインスペクション **SSL certificate-inspection**

ロギングオプション

許可トラフィックをログ **セキュリティイベント** **すべてのセッション**

セッション開始時にログを生成

パケットをキャプチャ

コメント 0/1023

このポリシーを有効化

図 4-8 IPv4 ポリシー設定

4.7. 動作確認

左メニュー「ログ&レポート」→「転送トラフィック」をクリックします。通常トラフィックが port1 経由での通信となっていることを確認することができます。

日付/時刻	送信元	宛先	宛先インターフェース	アプリケーション名	結果	ポリシー
2020/03/24 23:33:57	10.1.0.102	151.139.128.14 (ocsp.comodoca4.com)	port1	HTTP		lan-wan (1)
2020/03/24 23:33:57	10.1.0.102	4.2.2.2 (browsers.Level3.net)	port1	DNS	72 B / 124 B	lan-wan (1)
2020/03/24 23:33:57	10.1.0.102	185.184.8.30 (ams.creativecdn.com)	port1	HTTPS.BROWSER	UTM許可	lan-wan (1)
2020/03/24 23:33:57	10.1.0.102	4.2.2.2 (browsers.Level3.net)	port1	DNS	204 B / 104 B	lan-wan (1)
2020/03/24 23:33:57	10.1.0.102	4.2.2.2 (browsers.Level3.net)	port1	DNS		lan-wan (1)
2020/03/24 23:33:57	10.1.0.102	8.8.8.8 (dns.google)	port1	DNS	72 B / 124 B	lan-wan (1)
2020/03/24 23:33:57	10.1.0.102	8.8.8.8 (dns.google)	port1	DNS	67 B / 123 B	lan-wan (1)
2020/03/24 23:33:57	10.1.0.102	8.8.8.8 (dns.google)	port1	DNS	67 B / 99 B	lan-wan (1)
2020/03/24 23:33:57	10.1.0.102	8.8.8.8 (dns.google)	port1	DNS	70 B / 228 B	lan-wan (1)
2020/03/24 23:33:56	10.1.0.102	8.8.8.8 (dns.google)	port1	DNS	72 B / 104 B	lan-wan (1)
2020/03/24 23:33:56	10.1.0.102	8.8.8.8 (dns.google)	port1	DNS	72 B / 104 B	lan-wan (1)
2020/03/24 23:33:56	10.1.0.102	185.184.8.30 (ams.creativecdn.com)	port1	HTTPS.BROWSER	UTM許可	lan-wan (1)
2020/03/24 23:33:55	10.1.0.102	8.8.8.8 (dns.google)	port1	DNS	63 B / 79 B	lan-wan (1)
2020/03/24 23:33:55	10.1.0.102	52.168.140.71 (p1-px.trafficmanager.net)	port1	HTTPS	152 B / 0 B	lan-wan (1)
2020/03/24 23:33:55	10.1.0.102	4.2.2.2 (browsers.Level3.net)	port1	DNS	209 B / 121 B	lan-wan (1)
2020/03/24 23:33:55	10.1.0.102	4.2.2.2 (browsers.Level3.net)	port1	DNS		lan-wan (1)
2020/03/24 23:33:55	10.1.0.102	8.8.8.8 (dns.google)	port1	DNS	60 B / 121 B	lan-wan (1)
2020/03/24 23:33:53	10.1.0.102	8.8.8.8 (dns.google)	port1	DNS	62 B / 78 B	lan-wan (1)
2020/03/24 23:33:53	10.1.0.102	156.154.202.36 (aa.agkn.com)	port1	HTTPS.BROWSER	UTM許可	lan-wan (1)
2020/03/24 23:33:52	10.1.0.102	185.184.8.30 (ams.creativecdn.com)	port1	HTTPS.BROWSER	Deny-UTMブロック	lan-wan (1)
2020/03/24 23:33:52	10.1.0.102	23.142.112 (e13541.akamaiedge.net)	port1	HTTPS.BROWSER	Deny-UTMブロック	lan-wan (1)
2020/03/24 23:33:52	10.1.0.102	54.156.26.12 (ps.eyetia.net)	port1	HTTPS.BROWSER	Deny-UTMブロック	lan-wan (1)
2020/03/24 23:33:52	10.1.0.102	156.154.202.36 (aa.agkn.com)	port1	HTTPS.BROWSER	UTM許可	lan-wan (1)
2020/03/24 23:33:51	10.1.0.102	8.8.8.8 (dns.google)	port1	DNS	86 B / 102 B	lan-wan (1)
2020/03/24 23:33:51	10.1.0.102	8.8.8.8 (dns.google)	port1	DNS	69 B / 215 B	lan-wan (1)
2020/03/24 23:33:51	10.1.0.102	151.101.2 (api.taboola.com)	port1	HTTPS.BROWSER	Deny-UTMブロック	lan-wan (1)
2020/03/24 23:33:49	10.1.0.102	85.114.159.118 (isp.adfarm1.ladition.com)	port1	HTTPS.BROWSER	Deny-UTMブロック	lan-wan (1)

図 4-9 動作確認 (通常トラフィック)

検索ボックス内の「フィルタ追加」をクリックし、宛先をクリックします。先ほど登録した nhks-vh.akamaihd.net の IP アドレスを入力し、ログにフィルタをかけます。NHK for School トラフィックが port2 経由での通信となっていることを確認することができます。

日付/時刻	送信元	宛先	宛先インターフェース	アプリケーション名	結果	ポリシー
2020/03/24 23:54:39	10.1.0.102	23.35.111.34 (a6.w10.akamai.net)	port2	HTTPS.BROWSER	311.20 kB / 103.45 MB	lan-wan (1)
2020/03/24 23:52:39	10.1.0.102	23.35.111.34 (a6.w10.akamai.net)	port2	HTTPS.BROWSER	285.09 kB / 95.98 MB	lan-wan (1)
2020/03/24 23:50:38	10.1.0.102	23.35.111.34 (a6.w10.akamai.net)	port2	HTTPS.BROWSER	225.86 kB / 76.39 MB	lan-wan (1)
2020/03/24 23:48:37	10.1.0.102	23.35.111.34 (a6.w10.akamai.net)	port2	HTTPS.BROWSER	146.92 kB / 46.59 MB	lan-wan (1)
2020/03/24 23:46:37	10.1.0.102	23.35.111.34 (a6.w10.akamai.net)	port2	HTTPS.BROWSER	94.08 kB / 26.27 MB	lan-wan (1)
2020/03/24 23:44:46	10.1.0.102	23.35.111.34 (a6.w10.akamai.net)	port2	HTTPS.BROWSER	UTM許可	lan-wan (1)
2020/03/24 23:44:35	10.1.0.102	23.35.111.34 (a6.w10.akamai.net)	port2	HTTPS.BROWSER	45.24 kB / 11.47 MB	lan-wan (1)
2020/03/24 23:42:50	10.1.0.102	23.35.111.34 (a6.w10.akamai.net)	port2	HTTPS.BROWSER	UTM許可	lan-wan (1)
2020/03/24 23:42:49	10.1.0.102	23.35.111.34 (a6.w10.akamai.net)	port2	HTTPS.BROWSER	UTM許可	lan-wan (1)
2020/03/24 23:42:43	10.1.0.102	23.35.111.34 (a6.w10.akamai.net)	port2	HTTPS.BROWSER	UTM許可	lan-wan (1)
2020/03/24 23:42:41	10.1.0.102	23.35.111.34 (a6.w10.akamai.net)	port2	HTTPS.BROWSER	UTM許可	lan-wan (1)
2020/03/24 23:28:06	10.1.0.102	23.35.111.34 (a6.w10.akamai.net)	port2	HTTPS.BROWSER	UTM許可	lan-wan (1)
2020/03/24 23:27:04	10.1.0.102	23.35.111.34 (a6.w10.akamai.net)	port2	HTTPS.BROWSER	127.80 kB / 44.57 MB	lan-wan (1)
2020/03/24 23:25:08	10.1.0.102	23.35.111.34 (a6.w10.akamai.net)	port2	HTTPS.BROWSER	UTM許可	lan-wan (1)
2020/03/24 23:24:00	10.1.0.102	23.35.111.34 (a6.w10.akamai.net)	port2	HTTPS.BROWSER	UTM許可	lan-wan (1)
2020/03/24 23:21:28	10.1.0.102	23.35.111.34 (a6.w10.akamai.net)	port2	HTTPS.BROWSER	258.61 kB / 44.54 MB	lan-wan (1)
2020/03/24 23:20:16	10.1.0.102	23.35.111.34 (a6.w10.akamai.net)	port2	HTTPS.BROWSER	170.79 kB / 30.06 MB	lan-wan (1)

図 4-10 動作確認 (NHK for School)

* YouTube 通信はトラフィック検出時に動的に ISDB を作成します。そのため、各宛先の 2 度目の通信以降ブレイクアウトを行うことが可能です。

5. Appendix: スタティックルートによるインターネットブレイクアウト

NHK for School トラフィックは、「SD-WAN ルールによるインターネットブレイクアウト」の代わりにスタティックルート設定でもインターネットブレイクアウトが実現可能です。設定方法を記載します。

5.1. スタティックルートの設定

左メニュー「ネットワーク」→「スタティックルート」をクリックし、「新規作成」をクリックします。

ダイナミックゲートウェイ：有効

宛先：名前付きアドレス → NHK1

インターフェース：port2

ゲートウェイアドレス：ダイナミック

アドミニストレーティブ・ディスタンス：10

コメント：任意

ステータス：有効化済み



図 5-1 スタティックルートの設定 1

同じ手順でもう一つのドメインの設定を行います。

ダイナミックゲートウェイ：有効

宛先：名前付きアドレス → NHK2

インターフェース：port2

ゲートウェイアドレス：ダイナミック

アドミニストレーティブ・ディスタンス：10

コメント：任意

ステータス：有効化済み



図 5-2 スタティックルートの設定 2

5.2. IPv4 ポリシーの設定

「SD-WAN ルールによるインターネットブレイクアウト」と同様の設定です。

5.3. 動作確認

「SD-WAN ルールによるインターネットブレイクアウト」と同様の方法で確認可能です。

改定履歴

バージョン	リリース日	改定履歴
1.0.0	2020.4	初版発行
1.0.1	2020.4	「IPv4 ポリシー設定」の修正、「SD-WAN 向けインターフェーススタティックルートの設定」を追記、その他文言修正
1.0.2	2020.5	ISDB 更新に伴う修正