「セキュリティ屋の」AWS上で動くUTMの話

～UTMデビューの方からUTMエキスパートの方まで～

小野　克浩
Security Architect, IaaS

SOPHOS

SOPHOS

ソフォスについて

ソフォス・スナップショット

1985
オックスフォードで創業

$450M
2015年度
(APPX.)

2,500
従業員数
(APPX.)

HQ
オックスフォード
イギリス

200,000+
顧客

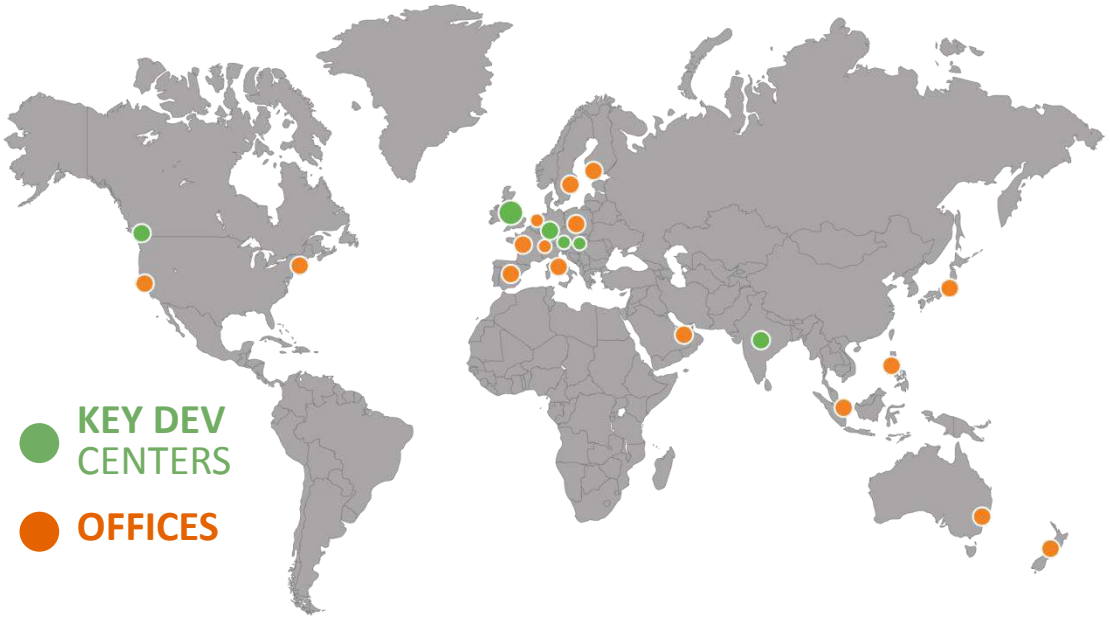
100M+
ユーザ数

90+%
更新率

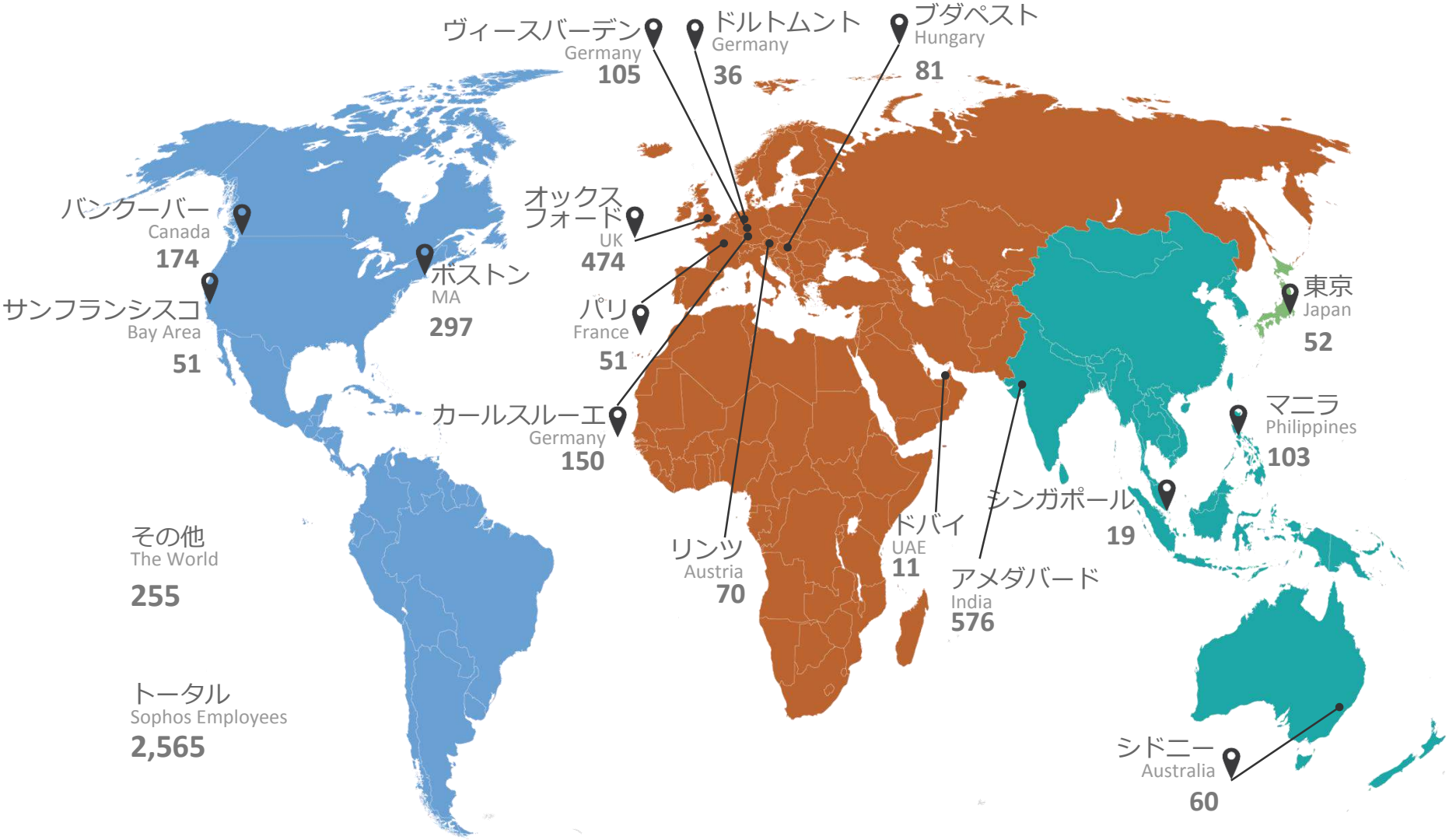
15,000+
チャネルパートナー

OEM パートナー:

CISCO
IBM
JUNIPER NETWORKS
lenovo
CITRIX
rackspace



ソフォス拠点一覧


ヴィースバーデン
Germany
105
ドルトムント
Germany
36
ブダペスト
Hungary
81
バンクーバー
Canada
174
オックスフォード
UK
474
ボストン
MA
297
サンフランシスコ
Bay Area
51
パリ
France
51
東京
Japan
52
カールスルーエ
Germany
150
マニラ
Philippines
103
シンガポール
19
ドバイ
UAE
11
リンツ
Austria
70
アメダバード
India
576
その他
The World
255
トータル
Sophos Employees
2,565
シドニー
Australia
60

新たなセキュリティリーダーとして

多様なセキュリティ
製品を幅広く提供

互いの情報を認識した
統合されたセキュリティ

シンプルで見やすい
デザイン

パートナー
チャネルファースト

個人向け無償製品の
提供

中小企業の予算で大
企業レベルのセキュリ
ティ対策を

SOPHOS

AWSで利用できるソフォス製品

AWS Marketplace で”Sophos”で検索

awsmarketplace

Amazon Web Services Home

Sign in or Create a new account

Your Account | Help | Sell on AWS Marketplace

Shop All Categories ▾ sophos GO Your Software

Categories

All Categories

Software Infrastructure (7)

Filters

Operating System

+ All Linux/Unix

Software Pricing Plans

- Free (2)
- Hourly (2)
- Annual (2)
- Bring Your Own License (2)

Software Free Trial

- Free Trial (2)

Delivery Method

- Amazon Machine Image (6)
- CloudFormation Stack (5)
- SaaS (1)

Average Rating

- ★★★★★ & up (1)
- ★★★★★ & up (2)
- ★★★★★ & up (2)
- ★★★★★ & up (2)

Architecture

- 64-bit (6)

Region

- US East (N. Virginia) (6)
- US West (Oregon) (6)

sophos (7 results) showing 1 - 7

SOPHOS

Free Trial

Sophos UTM 9

★★★★★ (10) | Version 9.313 | Sold by Sophos

Starting from $0.00/hr or from $789/yr (up to 18% savings) for software + AWS usage fees

A complete security platform for Amazon Web Services (AWS) Secure your AWS EC2 instances and VPCs with Sophos Unified Threat Management (UTM) for AWS. Its your complete ...

Linux/Unix, Other 9.3 | 64-bit Amazon Machine Image (AMI)

SOPHOS

Sophos UTM 9 (BYOL)

★★★★★ (5) | Version 9.313 | Sold by Sophos

Bring Your Own License + AWS usage fees

A complete security platform for Amazon Web Services (AWS) Secure your AWS EC2 instances and VPCs with Sophos Unified Threat Management (UTM) for AWS. Its your complete ...

Linux/Unix, Other 9.3 | 64-bit Amazon Machine Image (AMI)

Sophos Secure OS (CentOS)

Version 9.8.3 | Sold by Sophos

$0.00/hr for software + AWS usage fees

Sophos Secure OS makes it simple to deploy a secure server environment within Amazon Web Services. Within a single AMI, it combines CentOS with a preconfigured installation ...

Linux/Unix, CentOS 6.6 | 64-bit Amazon Machine Image (AMI)

SOPHOS

Free Trial

Sophos UTM 9 Autoscaling

Version 9.316 | Sold by Sophos

Starting from $0.065/hr or from $570/yr (up to 35% savings) for software + AWS usage fees

*** This product is intended to be deployed via cloudformation template (Template link is

検索しなくても大丈夫！

awsmarketplace

Amazon Web Services Home

Sign in or Create a new account

Your Account | Help | Sell on AWS Marketplace

Shop All Categories

Search AWS Marketplace GO

Your Software

Desktop Apps
Software Infrastructure
Application Development
Application Servers
Application Stacks
Big Data
Databases & Caching
Network Infrastructure
Operating Systems
Security
Developer Tools
Issue & Bug Tracking
Monitoring
Source Control
Testing
Business Software
Business Intelligence
Financial Services
Collaboration
Content Management
CRM
eCommerce
Education & Research
High Performance Computing
Media
Project Management
Storage & Backup

Product Demos
AWS Test Drive
try it now free

Build, Ship, Run Docker
Scalable | Reliable | Distribute
FREE 30 DAY TRIAL

Featured Products

WebSphere Application Server Base Edi...
MidVision Limited
$0.50 to $16.00/hr for software + Charges for EC2 with RHEL

Matillion ETL for Redshift
Matillion
Starting from $1.37/hr or from $10,200/yr for software
Free Trial

TIBCO Clarity
TIBCO Software, Inc.
Starting from $0.25/hr or from $1,095/yr for software
Free Trial

Popular Products

Sophos UTM 9
Sophos
Starting from $0.00/hr or from $789/yr for software
Free Trial

SoftNAS Cloud Standard - High-Perform...
SoftNAS
Starting from $0.00/hr or from $710/yr for software
Free Trial

TIBCO Jaspersoft for AWS with Multi-T...
TIBCO Software, Inc.
$0.90 to $26.16/hr for software

New Product Spotlight

Tableau Server (10 users)
Tableau
$0.63/hr or $5,500/yr for software + Charges for EC2 with Windows

Informatica Cloud Advanced for Amazon...
Informatica
$50.00/hr or $2,400/yr for software + Charges for EC2 with SUSE

Sophos UTM 9 Autoscaling
Sophos
Starting from $0.065/hr or from $570/yr for software
Free Trial

Popular Products

Sophos UTM 9
Sophos
Starting from $0.00/hr or from $789/yr for software
Free Trial

SoftNAS Cloud Standard - High-Perform...
SoftNAS
Starting from $0.00/hr or from $710/yr for software
Free Trial

TIBCO Jaspersoft for AWS with Multi-T...
TIBCO Software, Inc.
$0.90 to $26.16/hr for software

Oracle Linux 6.6
Orbitera - Oracle
Starting from $0.06/hr or

New Product Spotlight

Tableau Server (10 users)
Tableau
$0.63/hr or $5,500/yr for software + Charges for EC2 with Windows

Informatica Cloud Advanced for Amazon...
Informatica
$50.00/hr or $2,400/yr for software + Charges for EC2 with SUSE

Sophos UTM 9 Autoscaling
Sophos
Starting from $0.065/hr or from $570/yr for software
Free Trial

“Security”カテゴリでも

awsmarketplace

Amazon Web Services Home

Sign in or Create a new account

Your Account | Help | Sell on AWS Marketplace

Shop All Categories ▾ Search AWS Marketplace GO Your Software

Categories

All Categories

Software Infra

Security

Hourly (147)
Monthly (8)
Annual (80)
Bring Your Own License (63)

Software Free Trial
Free Trial (90)

Delivery Method
Amazon Machine Image (228)
CloudFormation Stack (13)
SaaS (100)

Average Rating
★★★★★ & up (49)
★★★★★ & up (59)
★★★★★ & up (61)
★★★★★ & up (61)

Architecture
32-bit (12)
64-bit (216)

Region
US East (N. Virginia) (229)
US West (Oregon) (226)
US West (N. California) (228)
EU (Frankfurt) (171)
EU (Ireland) (221)
Show more

Instance Type
+ Micro Instances (Free Tier)
+ General Purpose
+ Memory Optimized
+ Storage Optimized
+ Compute Optimized
+ GPU Instances

SOPHOS
Free Trial
Sophos UTM 9
★★★★★ (10) | Version 9.313 | Sold by Sophos
Starting from $0.00/hr or from $789/yr (up to 18% savings) for software + AWS usage fees
A complete security platform for Amazon Web Services (AWS) Secure your AWS EC2 instances and VPCs with Sophos Unified Threat Management (UTM) for AWS. Its your complete ...
Linux/Unix, Other 9.3 | 64-bit Amazon Machine Image (AMI)

Free Trial
The Security Technology Package (formerly Advanced Technology) of Cisco Cloud Services Router (CSR1000V) sets the standard for enterprise-class VPN in the AWS cloud, bringing ...
Linux/Unix, Other Cisco IOS XE | 64-bit Amazon Machine Image (AMI)

ALERT LOGIC
Free Trial
Alert Logic Threat Manager for AWS
★★★★★ (19) | Version 1.3* | Sold by Alert Logic, Inc.
Starting from $0.58/hr or from $4,050/yr (20% savings) for software + AWS usage fees
Alert Logic Threat Manager for AWS is a network intrusion detection service (IDS) specifically designed for AWS. This service allows you to cost-effectively protect the ...
Linux/Unix, CentOS 6.3 | 64-bit Amazon Machine Image (AMI)

TREND MICRO
Free Trial
Trend Micro Deep Security
★★★★★ (1) | Version Deep Security 9.6.2980 | Sold by Trend Micro
Starting from $1.50/hr or from $8,670/yr (34% savings) for software + AWS usage fees
Get proactive protection for your AWS workloads with Trend Micro Deep Security. Prevent network attacks or breaches with intrusion detection & prevention (IDS/IPS); virtually ...
Linux/Unix, Amazon Linux Amazon Linux 2014.09.1 x64 | 64-bit Amazon Machine Image (AMI)

f5
Free Trial
F5 BIG-IP Virtual Edition 200Mbps Best
★★★★★ (1) | Version 11.6.0.4.0.420-HF4 | Sold by F5 Networks
$2.50/hr or $13,797/yr (37% savings) for software + AWS usage fees
The BIG-IP Virtual Edition (VE) is the industry-leading application delivery services platform that ensures your business critical applications and network is fast, available, ...
Linux/Unix, CentOS 6.4 | 64-bit Amazon Machine Image (AMI)

FORTINET
Free Trial
Fortinet FortiGate-VM
★★★★★ (2) | Version v5.0.9 | Sold by Fortinet, Inc.
Starting from $0.30/hr or from $1,992/yr (up to 24% savings) for software + AWS usage fees
Fortinet FortiGate-VM firewall technology delivers complete content and network protection by

SOPHOS

Sophos UTM とは

Sophos UTM のセキュリティ機能

■ エンタープライズクラスのセキュリティをあらゆる規模の企業へ

エンドポイント プロテクション

- アンチウイルス
- HIPS
- デバイスコントロール
- Webコントロール

※Windowsのみをサポート
※BYOLのみ利用可

optional

ワイヤレス プロテクション

- ワイヤレスコントローラー
- マルチゾーン(SSID)サポート
- キャプティブポータル

optional

基本機能 (Essential Firewall)

- ステートフルファイアウォール
- NAT
- PPTP/L2TPリモートアクセス
- DNS/DHCP/NTPサーバ

optional

ネットワーク プロテクション

- IPS（侵入防御システム）
- IPSec/SSL VPN、RED
- ATP（標的型攻撃対策）
- HTML5 VPN

optional

Webサーバ プロテクション

- リバースプロキシ
- 認証リバースプロキシ
- WAF
- デュアルアンチウイルス

optional

メール プロテクション

- アンチスパム/フィッシング
- デュアルアンチウイルス
- メール暗号化

optional

Web プロテクション

- URLフィルタリング
- デュアルアンチウイルス
- スパイウェア
- アプリケーション制御

優れたユーザビリティ

- 直感的で容易な使い勝手を実現

1. 直感的なウェブインタフェース
2. 標準搭載のレポートツール
3. 自動設定によるHA/クラスタ
4. ワンクリック VPN
5. HTML5 VPN　ポータル
6. 無償の集中管理ツール（SUM）
7. 専用USBによる高速な障害復旧
8. 多言語対応のユーザポータル
9. ActiveDirectory連携
10. 設定変更履歴の管理

優れたユーザビリティ

■ 直感的で容易な使い勝手を実現（管理コンソール）

検索

Dashboard for 月曜日 4月 1 2013 | 11:46:07

ダッシュボード
マネジメント
定義とユーザ
インタフェース＆ルーティング
ネットワークサービス
ネットワークプロテクション
Webプロテクション
メールプロテクション
エンドポイントプロテクション
ワイヤレスプロテクション
Webサーバプロテクション
REDマネジメント
サイト間VPN
リモートアクセス
ログとレポート
サポート
ログオフ

asgt.mydns.jp

モデル: ASG320
S/N: [1] 940400124-100100
ライセンスID: 112177
サブスクリプション: 基本機能
メールプロテクション
ネットワークプロテクション
Webプロテクション
Webサーバプロテクション
ワイヤレスプロテクション
エンドポイントアンチウイルス
Uptime: 3d 20h 27m

バージョン情報

ファームウェアバージョン: 9.006-5
パターンバージョン: 44070
最後のチェック: 4分前

リソース使用率

CPU	74%
RAM	85% of 1.0 GB
ログ領域	9% of 36.3 GB
データ領域	24% of 27.7 GB

本日の脅威に関する統計

I/F	名前	タイプ	設定	リンク	In	Out
all	All Interfaces				29.8 kbit	95.6 kbit
eth0	used in lag0	リンクアグリゲーション	-	Up	-	-
eth1	External	イーサネット	Up	Up	13.0 kbit	4.3 kbit
eth2	Office	イーサネット	Up	Up	16.8 kbit	91.2 kbit
eth3	HA/Cluster	イーサネット	Up	Down	0	0
eth4	ADSL	DSL (PPPoE)	Down	Down	0	0
eth5	DMZ	イーサネット	Down	Down	0	0
eth6	unused					
eth7	used in lag0	リンクアグリゲーション	-	Up	-	-
lag0	Internal	イーサネット	Up	Up	0	<0.1 kbit

現在のシステム設定

- ファイアウォールは 10 ルールでアクティブ
- 侵入防御はインアクティブ
- Webフィルタリングはアクティブ、0リクエストを本日処理
- ネットワーク可視化は、1 アプリケーション制御ルールでアクティブ
- FTPプロキシはインアクティブ
- SMTPプロキシはアクティブ、0 メールを処理、0 メールをブロック
- POP3プロキシはアクティブ、230 メールを処理、2 メールをブロック
- Webアプリケーションファイアウォールはインアクティブ
- アンチウイルスはプロトコル HTTP/S, SMTP, POP3 に対してアクティブ
- アンチスパムはプロトコル SMTP, POP3に対してアクティブ

優れたユーザビリティ

- 直感的で容易な使い勝手を実現（サマリーレポーティング）

SOPHOS Executive Report

日付: 2013/08/23
タイプ: daily

デバイス情報：

組織:	Sophos K.K.
国:	JP
市区町村:	Tokyo
シリアル番号:	00000000000-00000000
ライセンス ID:	000000
ホスト名:	utm.sophos.local
ファームウェアバージョン:	9.104-18
アップタイム:	24 日 2 時間 10 分

クイックリンク:
リソース使用状況 | ネットワーク使用状況 | Network Protection | Web Protection | Email Protection | アプリケーション コントロール | VPN

サマリー

ネットワーク使用状況:

処理したトラフィック:	120.2 GB
処理した接続:	2 567 597

Network Protection:

ファイアウォールでブロックされたパケット:	493 702
IPS でブロックした攻撃:	2 514

Web フィルタリング:

Web サイトのリクエスト総数:	87590
ブロックした URL	9512
ブロックした HTTP/S ウイルス	61
ブロックした HTTP/S マルウェア	4

メールフィルタリング:

処理したメール:	92425
ブロックしたスパムメール:	15201
ブロックしたウイルスメール:	256

VPN:

VPN 接続:	152
VPN トラフィック:	not accounted

WebAdmin ログイン:

成功:	57
失敗:	5

コンソール ログイン:

成功:	0
失敗:	0

Up2Date:

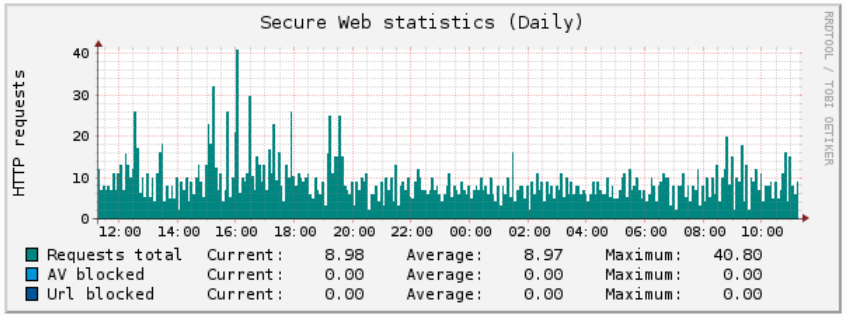
成功したリクエスト	146
失敗したリクエスト	3
インストール済ファームウェアアップデート版:	2
インストール済パターンアップデート:	19

システム:

システム再起動:	0
アップリンクのフェイルオーバー:	0
HA/クラスタ フェイルオーバー:	1

トップへ

Web Protection



Web 使用状況

時間ごとのユーザ トップ10

	ユーザ	時間	%
1	192.168.0.200	23:40:42	43.2 %
2	192.168.0.101	15:08:04	27.3 %
3	192.168.0.203	07:20:19	12.9 %
4	192.168.0.191	06:09:19	12.3 %
5	192.168.0.50	01:40:39	2.4 %
6	192.168.0.202	01:31:06	2.3 %
7	192.168.0.213	00:09:02	0.3 %
8	192.168.0.215	00:04:00	0.1 %
9	192.168.0.217	00:02:00	0.1 %

トラフィックごとのユーザ トップ10

	ユーザ	トラフィック	%
1	192.168.0.101	407.3 MB	66.5 %
2	192.168.0.200	20.9 MB	20.8 %
3	192.168.0.203	31.7 MB	5.1 %
4	192.168.0.191	22.0 MB	3.6 %
5	192.168.0.213	21.8 MB	3.6 %
6	192.168.0.215	1.5 MB	0.2 %
7	192.168.0.50	551.7 kB	0.1 %
8	192.168.50.202	441.4 kB	0.1 %
9	192.168.0.217	222.9 kB	0.0 %

時間ごとのドメイン トップ10

	ドメイン	時間	%
1	sophosxl.net	29:31:46	39.9 %
2	sophos.com	12:53:27	16.5 %
3	sophosupd.com	12:24:41	13.9 %
4	astaro.com	06:48:35	2.8 %
6	175.41.132.12	01:26:00	1.5 %
7	windowsupdate.com	01:25:39	1.5 %
8	accu-weather.com	01:15:00	0.9 %
9	microsoft.com:80	01:13:23	0.8 %
10	79.125.21.244	00:12:00	0.7 %

トラフィックごとのドメイン トップ10

	ドメイン	トラフィック	%
1	sophos.com	429.4 MB	70.1 %
2	astaro.com	62.3 MB	10.2 %
3	apple.com	31.7 MB	5.2 %
4	sophosupd.com	17.2 MB	2.8 %
5	175.41.132.12	16.9 MB	2.8 %
6	s-msn.com	13.2 MB	2.2 %
7	alc.co.jp	9.4 MB	1.5 %
8	microsoft.com	6.4 MB	1.0 %
9	msn.com	6.4 MB	1.0 %
10	accu-weather.com	2.5 MB	0.4 %

優れた防御力

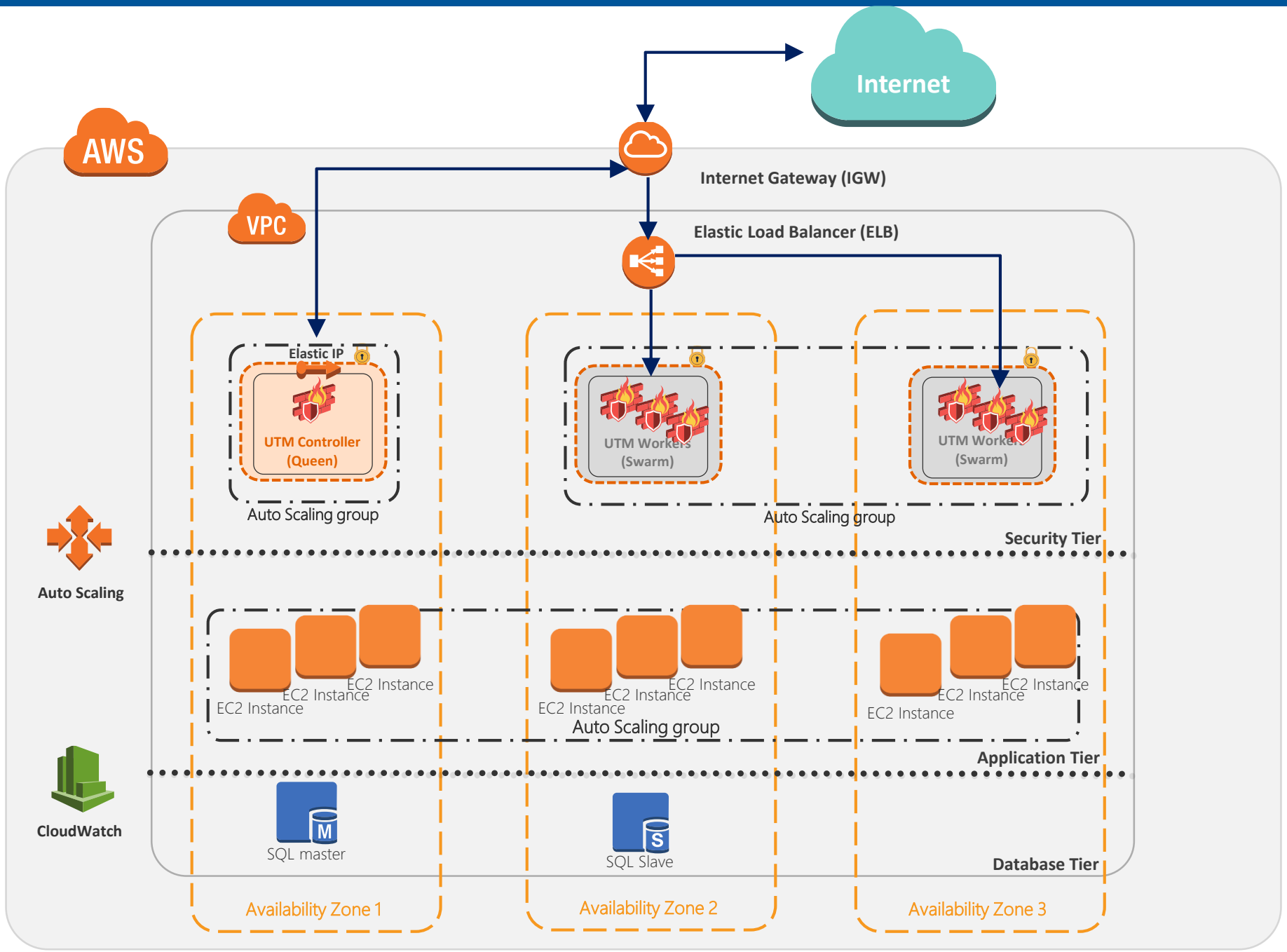
■ 特徴的なセキュリティ機能

SOPHOS AVIRA

1. デュアルアンチウイルスエンジン
2. RED –設定不要のVPN専用BOX
3. ワイヤレスコントローラの統合
4. Endpoint Protection管理の統合
5. NGFW （アプリケーション制御）
6. Web Application Firewall
7. Email暗号化（SPX,S/MIME,OpenPGP）
8. HTTPS通信のウイルススキャン
9. 主要なOSのVPN接続をサポート
10. クラウドでも全機能を提供可能

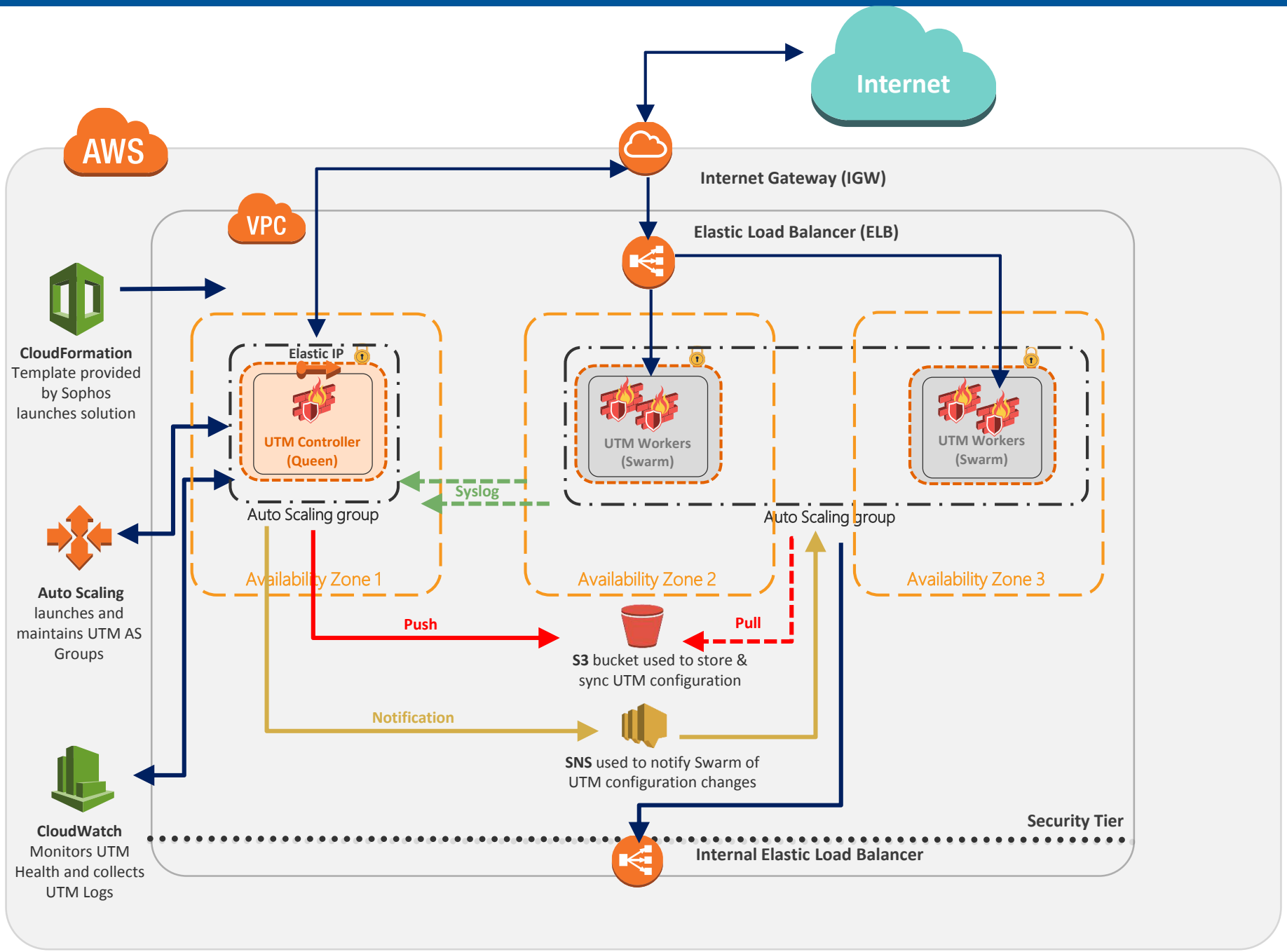
SOPHOS

AutoScaling Architecture on AWS


Internet
AWS
Internet Gateway (IGW)
VPC
Elastic Load Balancer (ELB)
Elastic IP
UTM Controller
(Queen)
Auto Scaling group
UTM Workers
(Swarm)
Auto Scaling group
UTM Workers
(Swarm)
Security Tier
Auto Scaling
EC2 Instance
EC2 Instance
EC2 Instance
EC2 Instance
EC2 Instance
EC2 Instance
EC2 Instance
EC2 Instance
EC2 Instance
Auto Scaling group
Application Tier
CloudWatch
SQL master
SQL Slave
Database Tier
Availability Zone 1
Availability Zone 2
Availability Zone 3

UTM AutoScaling は AWS Marketplaceから使用可能

- 冗長化によるSPOFの解消と、自動の伸縮性が実現
- Cloudformation テンプレートで素早くデプロイ
- ライセンス従量課金と BYOL に対応
- ソリューションの構成:
  - UTM Queen (controller) と Swarm (worker) ノード
  - ELB を使用したインバウンドWebトラフィック保護
  - S3 データストレージを使用した設定の保存
  - SNS を使用してSwarm ノードの設定変更
  - Queen と Swarm Auto Scaling グループ
  - Cloudwatch アラーム


Internet
AWS
Internet Gateway (IGW)
VPC
Elastic Load Balancer (ELB)
CloudFormation
Template provided by Sophos launches solution
Elastic IP
UTM Controller (Queen)
UTM Workers (Swarm)
UTM Workers (Swarm)
Syslog
Auto Scaling group
Auto Scaling group
Availability Zone 1
Availability Zone 2
Availability Zone 3
Auto Scaling
launches and maintains UTM AS Groups
Push
Pull
S3 bucket used to store & sync UTM configuration
Notification
SNS used to notify Swarm of UTM configuration changes
CloudWatch
Monitors UTM Health and collects UTM Logs
Security Tier
Internal Elastic Load Balancer

UTM on AWS ナレッジベース

Sophos UTM 9 Autoscaling Web Application Firewall の概要

https://www.sophos.com/ja-jp/support/knowledgebase/122742.aspx

Sophos UTM を Amazon Web Services VPC にコールドスタンバイまたはウォームスタンバイの冗長構成 (HA) で導入する手順

https://www.sophos.com/ja-jp/support/knowledgebase/122202.aspx

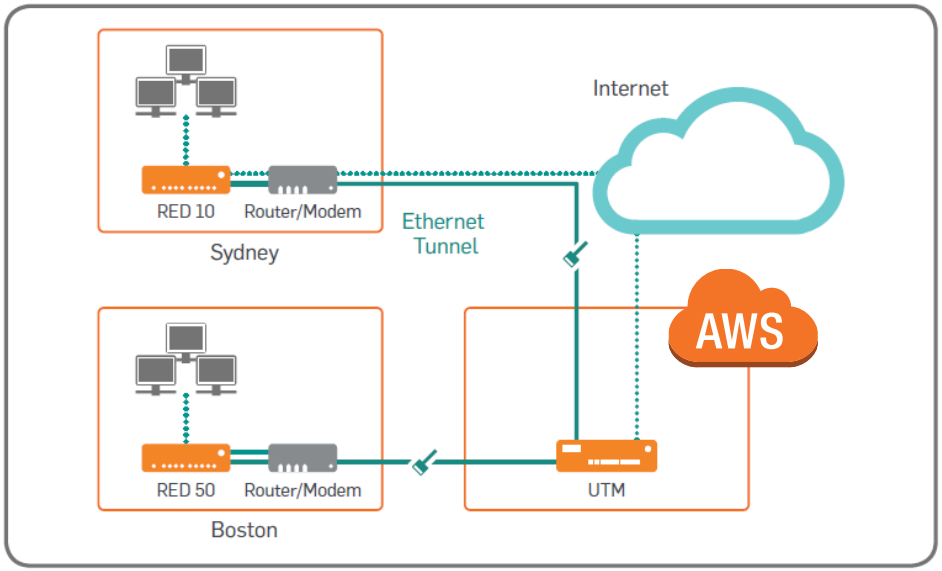
SOPHOS

Remote Ethernet Device

Sophos RED

支社・支店オフィスセキュリティー　シンプル、プラグ&プレイ

- セキュアなリモート接続
- 設定不要
- 柔軟な設置オプション
- 全てのオフィスに同じ保護
- 完全にトラヒックを暗号化
- UTMで集中管理
- 追加のライセンスや保守は不要
- トンネル圧縮 (15/50)
- セカンダリUTMの設定(15/50)



Sophos RED 選択のメリット

■ 拠点展開にREDを選択するメリット

- **機器設定が不要**
  - 新規設置時、拠点追加時に、予めRED本体に設定作業を行う必要がありません。
  - 故障時の交換部材に対してもRED本体に設定作業が発生しません。REDを正常品に交換し、本社UTMで機器IDの更新操作のみです。

- **セキュリティポリシーの一元管理**
  - REDを使用して拠点展開を行うことにより、ゲートウェイのアクセスポリシーを本社、拠点を問わず一元的に管理することが出来ます。

- **UTMの機能を拠点でも利用可能**
  - RED配下のネットワークは本社UTMの傘下となるため、UTM が提供する様々な機能を利用することが可能です。例えば、DHCPサービス、DNSサービス、無線LANサービスも本社UTMで一元管理可能です。

Sophos RED の機器仕様

■ 製品仕様

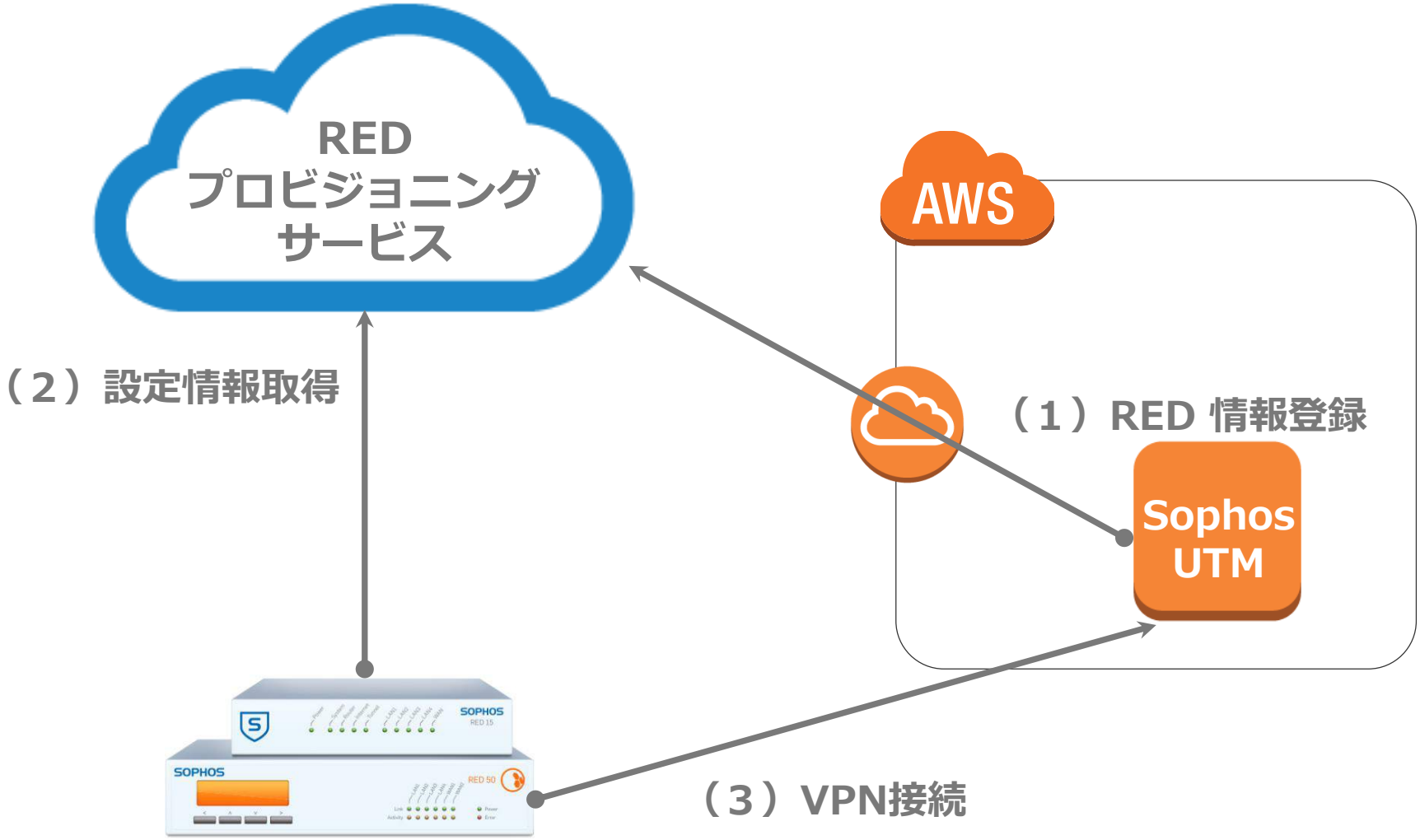
上段: Sophos RED 15
下段: Sophos RED 50

容量/型番	RED15	RED50
最大ユーザ数	無制限	
最大スループット	90Mbps	360Mbps
物理インターフェース		
LAN	4×10/100/1000BASE-TX（スイッチ）	4×10/100/1000BASE-TX（スイッチ）
WAN	1×10/100/1000BASE-TX、1×USB	2×10/100/1000BASE-TX、2×USB
電源	AC110～240V、 50～60Hz、最大1.5A	AC100～240V、 50～60Hz、1.3A

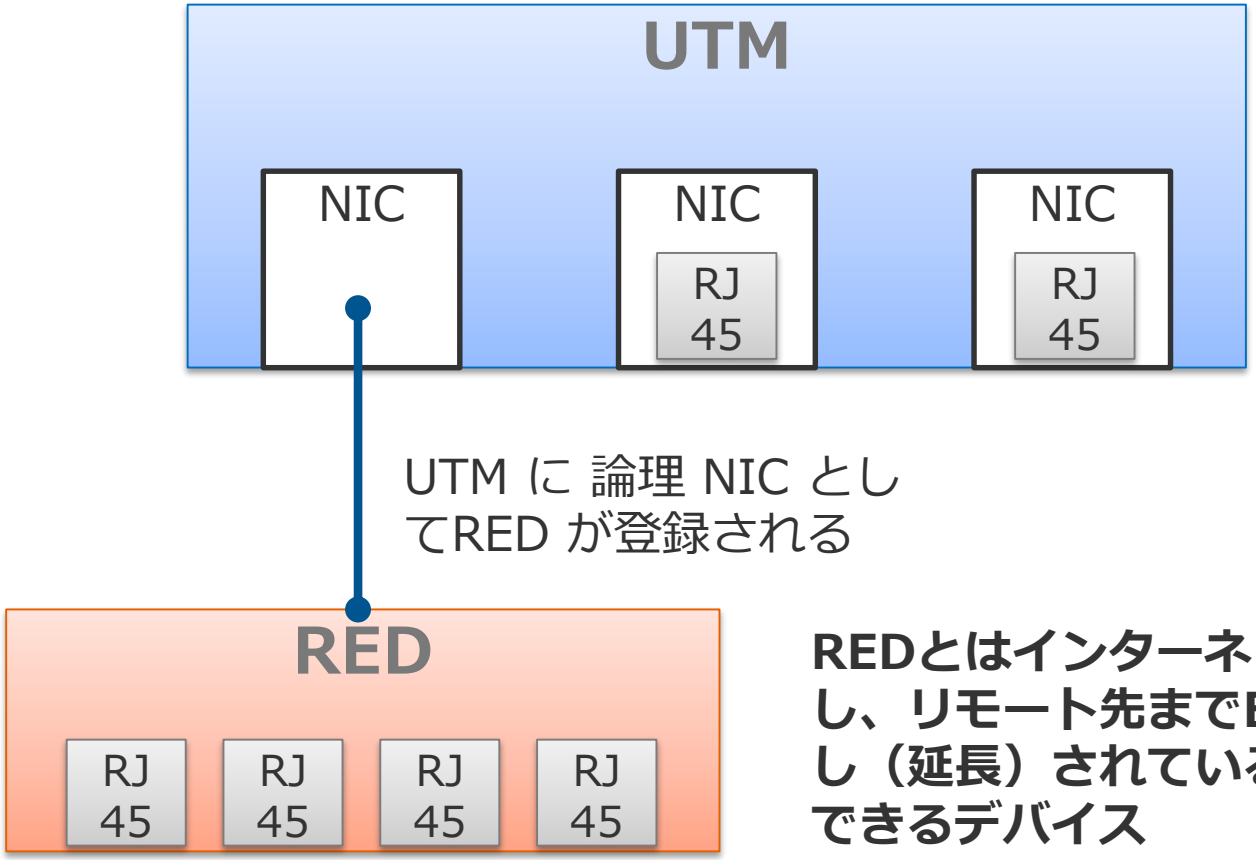
SOPHOS

UTMとREDの仕組み

オンラインプロビジョニング：３ステップ



RED 論理イメージ



REDとはインターネットVPNを使用し、リモート先までEthernetが張出し（延長）されているイメージが実現できるデバイス

Remote **E**thernet **D**evice

RED VPN接続形態

- RED10
  - シングルセッションの接続に対応
- RED 15
  - UTM 障害時のフェールオーバーモードの設定が可能
- RED 50
  - UTM と RED WAN 障害時のフェールオーバーモード
  - NWロードバランシングの設定が可能、
    - UTM hostname = Failover / RED uplink = Failover
    - UTM hostname = Balancing / RED uplink = Failover
    - UTM hostname = Failover / RED uplink = Balancing
    - UTM hostname = Balancing / RED uplink = Balancing
- UTM
  - REDトンネル接続をサポート

REDの使用ポート

- RED 10 で使用されるポート
  - 3400/tcp （制御接続、SSL 使用、X509 相互認証証明書チェックで認証）
  - 3400/udp （カプセル化トラフィック、AES256 (enc)、SHA1-HMAC (auth)）

- RED 15/50 で使用されるポート
  - 3400/tcp （制御接続、SSL 使用、X509 相互認証証明書チェックで認証）
  - 3410/udp （カプセル化トラフィック、AES256 (enc)、SHA1-HMAC (auth)）

RED の登録画面：RED 10

REDタイプ: RED 10

ブランチ名:

これはREDを設置するリモートサイトを短く記述する名前(例えばOffic
Branch 42nd streetなど)です。

UTM ホスト名:

UTMホスト名は、このUTMのパブリックに解決可能なDNS名かIPアド
す。REDはこの名前/IPを使用してUTMに接続します。

RED ID #:

RED IDはREDの裏面に貼付されたステッカーに印字された15文字の
(左の画像参照)。パッケージを開封したくない場合は、外箱のステッカーにも印字さ
れています。

ロック解除コード(オプション):

「ロック解除コード」は、REDがUTMに追加される際に生成される 8文字の文字列で
す。このREDを今はじめて導入する場合は、ロック解除コードは不要
したことがある場合は、ここでロック解除コードを入力する必要があり

REDに付加するタグ情報（任意の文字可）

REDがVPN接続をおこなう先のUTMのFQDN/IPアドレス情報

RED本体に印字されているRED IDを入力

REDを登録時に生成され、管理者メールアドレスにも送信されます

※[重要]：ロック解除コードが不明となった場合はサポートまでお問合せください

RED の登録画面：RED 15/50

REDタイプ: RED 50

ブランチ名:

これはREDを設置するリモートサイトを短く記述する名前(例えばOffice MunichやBranch 42nd streetなど)です。

UTM ホスト名:

UTMホスト名は、このUTMのパブリックに解決可能なDNS名かIPアドレスです。REDはこの名前/IPを使用してUTMに接続します。

第2UTMホスト名:

このUTMの第 2 DNSホスト名もしくはIPアドレスを設定できます。第2アップ
使用して別ルートを利用できます。

RED VPN接続のFailover/Balancing構成時に利用するUTMのFQDN/IPアドレス情報

RED ID #:

RED IDはREDの裏面に貼付されたステッカーに印字された15文字の文字列です(左の画像参照)。パッケージを開封したくない場合は、外箱のステッカーにも印字されています。

ロック解除コード(オプション):

「ロック解除コード」は、REDがUTMに追加される際に生成される 8文字の文字列です。このREDを今はじめて導入する場合は、ロック解除コードは不要です。以前導入したことがある場合は、ここでロック解除コードを入力する必要があります。

RED の登録画面：一覧

概要 | グローバル設定 | [サーバ] クライ... | [サーバ] 導入へ... | [クライアント] トン...

REDの追加

すべて

検索 検索

表示: 10

1-3 of 3

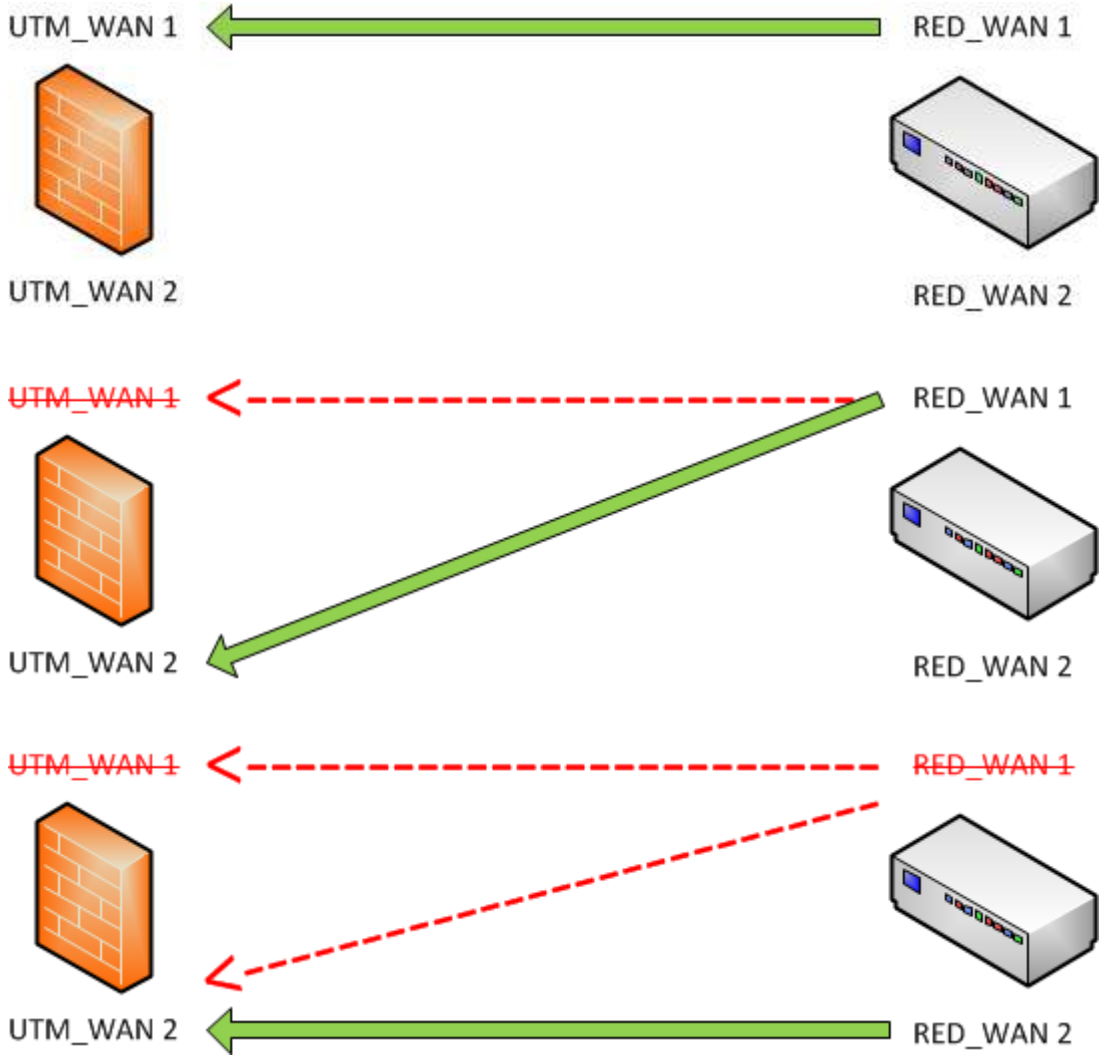
アクション	ステータス	タイプ	名前
編集 / 削除		UTM	reds3 (UTM-RED) RED ID: 7ab1486f1e60df1 トンネルID: 3 ダウンロードするプロビジョニングファイル: Download
編集 / 削除		RED 50	reds1 (AWS Demo) RED ID: A3400788A17CEA8 トンネルID: 1 ロック解除コード: cyylb0sq UTM ホスト名: ec2-54-64-246-87.ap-northeast-1.compute.amazonaws.com アップリンクモード: DHCP 第2アップリンクモード: DHCP 第2アップリンクの用途: Failover 操作モード: 標準/統合
編集 / 削除		RED 50	reds2 (RED010) RED ID: A34007DB78F3176 トンネルID: 2 ロック解除コード: zhk3ecqx UTM ホスト名: 54.65.162.114 アップリンクモード: DHCP 第2アップリンクモード: DHCP 第2アップリンクの用途: Failover 操作モード: 透過/分割

RED 50 冗長化モード

- Failover
  - WANインターフェース、UTMそれぞれのNWに障害発生時にフェールオーバーします
- Balancing
  - WANインターフェース、UTMそれぞれのアクティブ負荷分散を有効にできます。このオプションは負荷分散している両方のアップリンクと遅延が等しくない場合はお奨めできません。
- 3G/UMTS フェイルオーバー：※rev.2以降より
  - WANインターフェース側のNWに障害発生時、3G回線でのフェールオーバーに対応
  - GSM/CDMA方式に対応

RED 50冗長化（1）

UTM = Failover / RED = Failover



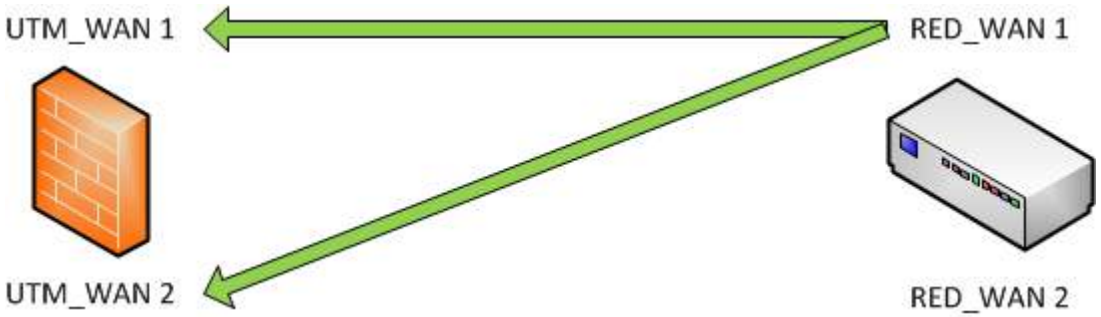
RED が RED_WAN1 および UTM_WAN1 間の接続を確立

UTM_WAN1 がダウンした場合、RED_WAN1 は UTM_WAN2 に接続

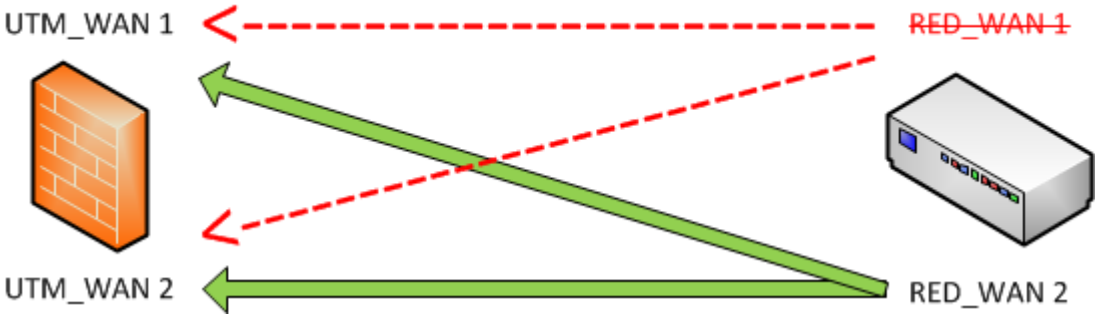
UTM_WAN1 および RED_WAN1 がダウンした場合、RED_WAN2 は UTM_WAN2 に接続

RED 50冗長化（2）

UTM = Balancing / RED = Failover



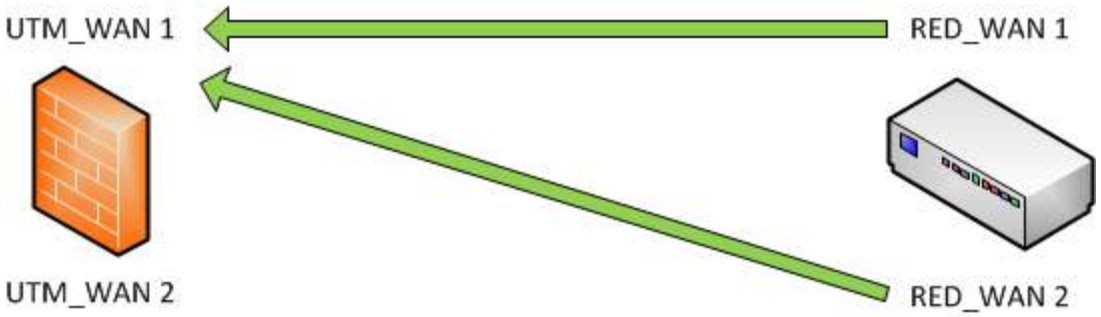
RED が RED_WAN1 および UTM_WAN1 / UTM_WAN2 間の接続を確立



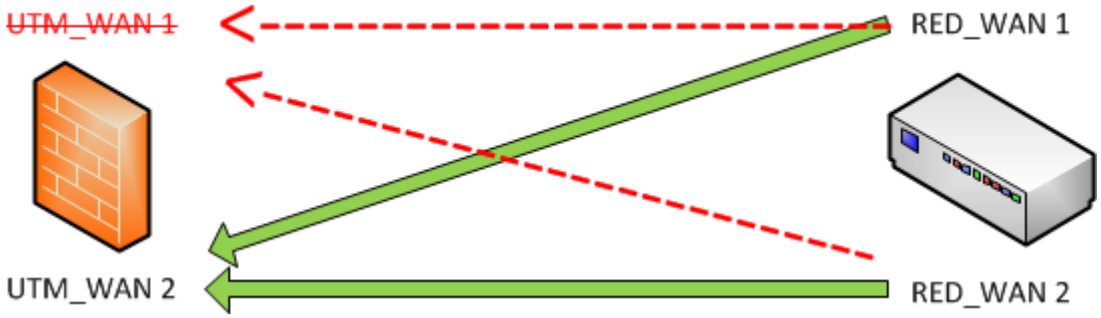
RED_WAN1 がダウンした場合、RED_WAN2 は UTM_WAN1 / UTM_WAN2 に接続

RED 50冗長化（3）

UTM = Failover / RED =Balancing



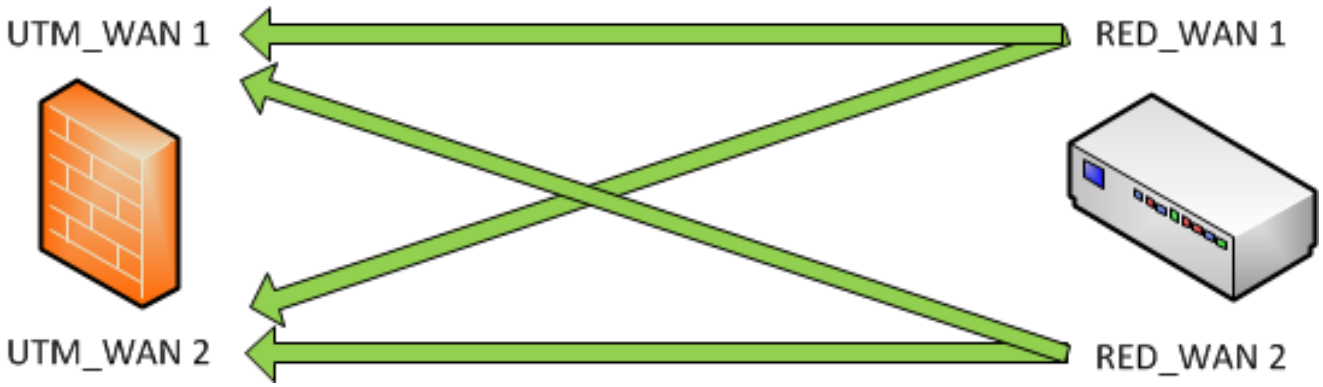
RED が RED_WAN1 / RED_WAN2 および UTM_WAN1 間の接続を確立



UTM_WAN1 がダウンした場合、RED_WAN1 / RED_WAN2 は UTM_WAN2 に接続

RED 50冗長化（4）

UTM = Balancing / RED =Balancing



RED が RED_WAN1 / RED_WAN2 および UTM_WAN1 / UTM_WAN2 間の接続を確立

注※： インタフェースのいずれかがダウンした場合、再び正常に機能するようになるまでそのインタフェースはチェックされます。インタフェースが回復した場合は、元のインタフェースに接続が復元されます。

SOPHOS

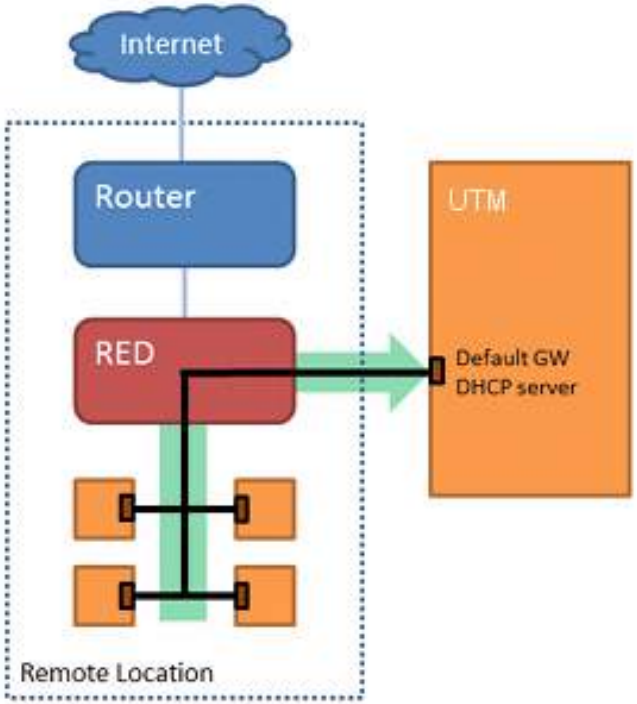
RED配下のNW設定

RED オペレーションモード：導入形態

- 標準／統合モード：
  - UTMがリモートネットワークを管理します。リモートネットワークのトラフィックは全てUTMに送信されます。
- 標準／分割モード：
  - UTMがリモートネットワークを管理、内部トラフィックのみがUTMを通して送信されます。
- 透過／分割モード：
  - リモートネットワークは変更されません。内部トラフィックのみUTMを通して送信されます。

RED オペレーションモード：標準／統合モード

導入形態の選択: 標準/統合:UTMがリモートネットワークを管理します。リモートネットワークのトラフィックは全てU ▼



標準: DHCPサーバ及びデフォルトゲートウェイとして動作することにより、UTMがリモートネットワークを管理します。リモートネットワークのトラフィックは全てUTMに送信されます。

RED インタフェース IPv4:

ネットマスク: /24 (255.255.255.0) ▼

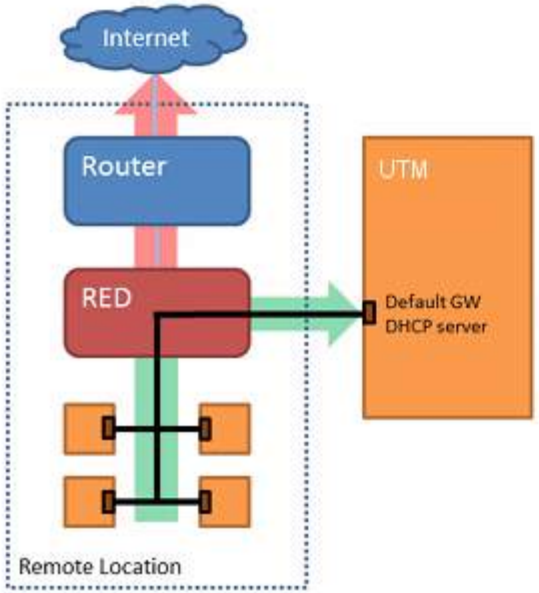
リモートネットワーク上でUTMインタフェースが使用するIPアドレスおよびネットマスクを入力してください。システムは自動的に次のものを設定します。

- 指定されたIPアドレスのローカルインタフェース
- 利用可能なレンジ内の半数のアドレスをカバーするリモートネットワーク向けDHCPサーバ
- リモートネットワーク向けのローカルDNSリゾルバ

全ての設定は各設定ページにて後で変更が可能です。なお、自動セットアップ後、リモートネットワークから他のネットワークやインターネットへの通信のために、ファイアウォール(および必要に応じたマスカレード)ルールの追加が必要ですのでご注意ください。

RED オペレーションモード：標準／分割モード

導入形態の選択: 標準/分割: UTMがリモートネットワークを管理、内部トラフィックのみがUTMを通して送信されま ▼



標準/分割(Standard/Split): DHCPサーバおよびデフォルトゲートウェイとして動作することにより、UTMがリモートネットワークを管理します。下で指定されたネットワークに対するトラフィックのみがUTMに送信されます。その他のトラフィックはすべてインターネットに直接送信されます。

RED インタフェース IPv4:

ネットマスク: /24 (255.255.255.0) ▼

リモートネットワーク上でUTMインタフェースが使用するIPアドレスおよびネットマスクを入力してください。システムは自動的に次のものを設定します。

- 指定されたIPアドレスのローカルインタフェース
- 利用可能なレンジ内の半数のアドレスをカバーするリモートネットワーク向けDHCPサーバ
- リモートネットワーク向けのローカルDNSリゾルバ

全ての設定は各設定ページにて後で変更が可能です。なお、自動セットアップ後、リモートネットワークから他のネットワークへの通信のために、ファイアウォール(および必要に応じたマスカレード)ルールの追加が必要ですのでご注意ください。

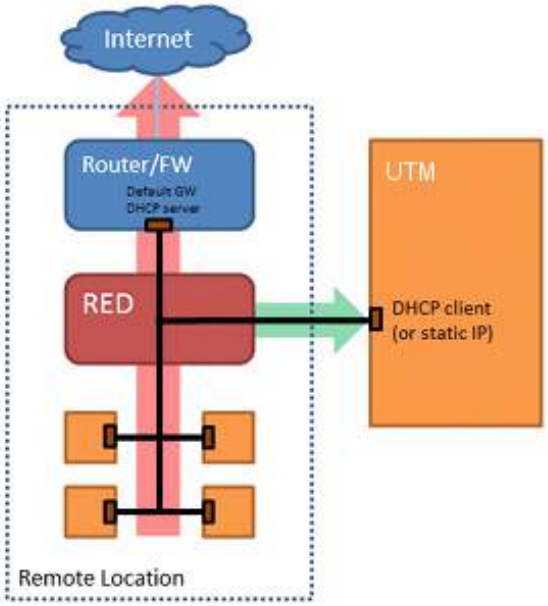
ネットワークの分割

DND DND DND D
DND DND DND
DND DND DND D

これはUTMにリダイレクトされるネットワークのリストです。他のネットワーク宛のトラフィックは通常のデフォルトゲートウェイ経由のままとなります。

RED オペレーションモード：透過／分割モード

導入形態の選択: 透過/分割: リモートネットワークは変更されません。内部トラフィックのみがUTMを通して送信され ▼



透過/分割(Transparent/Split): UTMはリモートネットワーク全体を管理しません。ただし、UTMはDHCPを使用してリモートネットワークからIPアドレスを要求することにより、リモートネットワークに属します。下で指定されたネットワークに対するトラフィックのみがUTMに転送されます。

ネットワークの分割

これはUTMにリダイレクトされるネットワークのリストです。他のネットワーク宛のトラフィックは通常のデフォルトゲートウェイ経由のままとなります。

分割DNSサーバ:

分割ドメイン

オプション: **分割DNSサーバ**経由で解決したい**分割ドメイン**のリストを指定してください。他の全てのドメインはリモートサイトで使用されている標準DNSサーバにより解決されます。

Switch port 設定

- REDのLANポートのモード設定は以下のとおり

- LANポートモード：
  - Switch：全トラフィックがすべてのポートに送信されます

  - VLAN：イーサネットのフレームのVLANタグに従ってトラフィックをフィルタリングすることが可能なため、複数のネットワークをRED トンネルでトンネル化することが可能です

RED 設定情報：詳細

REDの編集

ブランチ名: reds1 (AWS Demo)
クライアントタイプ: RED 50
RED ID#: A3400788A17CEA8
トンネルID: 1
ロック解除コード: cyylb0sq
UTM ホスト名: ec2-54-64-246-87.ap-northea
第2UTMホスト名:
第2ホスト名の用途: フェイルオーバ
アップリンクモード: DHCPクライアント
2つ目のアップリンク... DHCPクライアント
第2アップリンクの用途: フェイルオーバ
オペレーションモード: 標準/統合

Switch port 設定

LANポートモード: Switch

詳細

設定されたMACアドレスのリストが見つかりません。

デバイスの導入: 自動 (プロビジョニングサービス経由)

トンネル内通信を圧縮

3G/UMTSフェイルオ...

保存 キャンセル

アクション	ステータス	タイプ	名前
編集 / 削除		RED 50	reds1 (AWS Demo)

RED ID: A3400788A17CEA8
トンネルID: 1
ロック解除コード: cyylb0sq
UTM ホスト名: ec2-54-64-246-87.ap-northeast-1.compute.amazonaws.com
アップリンクモード: DHCP
第2アップリンクモード: DHCP
第2アップリンクの用途: Failover
操作モード: 標準/統合

参考情報：RED設定・構築

- Sophos RED (Remote Ethernet Device) Technical Training Guide
  http://www.sophos.com/ja-jp/support/knowledgebase/116573.aspx

- RED 50 の設定方法
  http://www.sophos.com/ja-jp/support/knowledgebase/118916.aspx

- How to configure Site-to-Site RED Tunnels
  http://www.sophos.com/ja-jp/support/knowledgebase/120157.aspx

- How to create Site-to Site RED full tunnels
  http://www.sophos.com/ja-jp/support/knowledgebase/120263.aspx

SOPHOS

AWS環境向けお奨め利用シーンのご紹介

ファイアウォール｜送受信国別ブロック

GeoIP ロケーションによる送受信国別ブロック

SOPHOS UTM 9 | admin |

検索

ファイアウォール

- ダッシュボード
- マネジメント
- 定義とユーザ
- インタフェースとルーティング
- ネットワークサービス
- ネットワークプロテクション
  - ファイアウォール
  - NAT
  - 高度な脅威防御(ATP)
  - 侵入防御(IPS)
  - サーバロードバランシング
  - VoIP
  - 詳細
- Webプロテクション
- Eメールプロテクション
- エンドポイントプロテクション
- ワイヤレスプロテクション
- Webサーバプロテクション
- REDマネジメント
- サイト間VPN
- リモートアクセス
- ログとレポート

ルール | 送受信国別... | 送受信国除外 | ICMP | 詳細

送受信国ブロックステータス

国

送信元・宛先国別にトラフィックを完全にブロックしたい場合、1つ以上の国を選択してください。送受信国別ブロックは、ポートフォワーディングやメールのルーティングなど他のセキュリティ機能が適用される前に、全てのトラフィックをブロックします。

--- North America

OFF Anguilla	OFF El Salvador	OFF Panama
OFF Antigua and Barbuda	OFF Greenland	OFF Puerto Rico
OFF Aruba	OFF Grenada	OFF Saint Barthelemey
OFF Bahamas	OFF Guadeloupe	OFF Saint Kitts & Nevis Anguilla
OFF Barbados	OFF Guatemala	OFF Saint Lucia
OFF Belize	OFF Haiti	OFF Saint Martin (French)
OFF Bermuda	OFF Honduras	OFF Saint Pierre and Miquelon
OFF Canada	OFF Jamaica	OFF Saint Vincent & Grenadines
OFF Cayman Islands	OFF Martinique (French)	OFF Trinidad and Tobago
OFF Costa Rica	OFF Mexico	OFF Turks and Caicos Islands
OFF Cuba	OFF Montserrat	OFF United States
OFF Dominica	OFF Netherlands Antilles	OFF Virgin Islands (British)
OFF Dominican Republic	OFF Nicaragua	OFF Virgin Islands (USA)

--- South America

OFF Argentina	OFF Ecuador	OFF Peru

Amazon WorkSpaces での出口対策

マルウェアの防御と*URL*フィルタを提供します

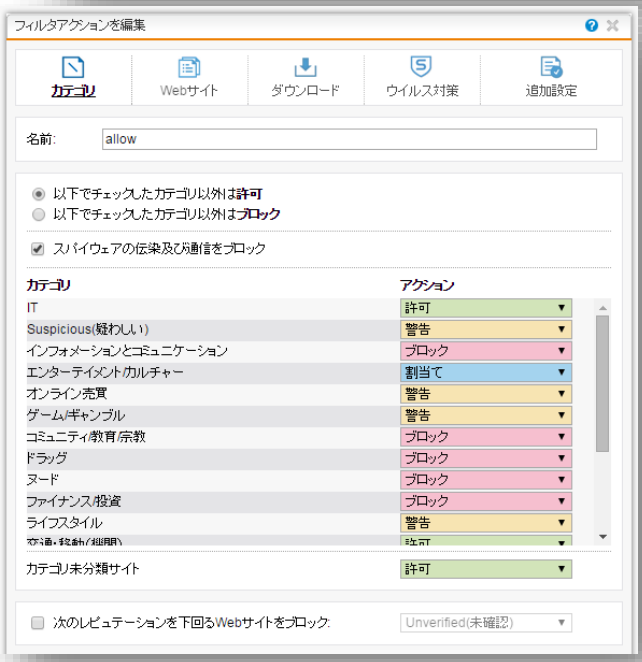
- HTTP、HTTPS、FTPトラフィックを監視、制限
- Webアプリケーションへのアクセスを管理
- 複数のプロファイルとポリシーをサポート

マルウェアのプロテクション

- ウィルス・トロイ・スパイウェアなどをブロック
- デュアルエンジン（Sophos・Avira）を利用
- スパイウェアで利用されるURLをブロック
- ファイルタイプからダウンロードをブロック

URLフィルタ

- 100以上のカテゴリごとにWebアクセスを制限
- 各Webサイトの世の中での脅威の程度を考慮
- ローカルでの再分類
- ホワイトリストとブラックリストの追加
- 複数のユーザー認証オプションをサポート



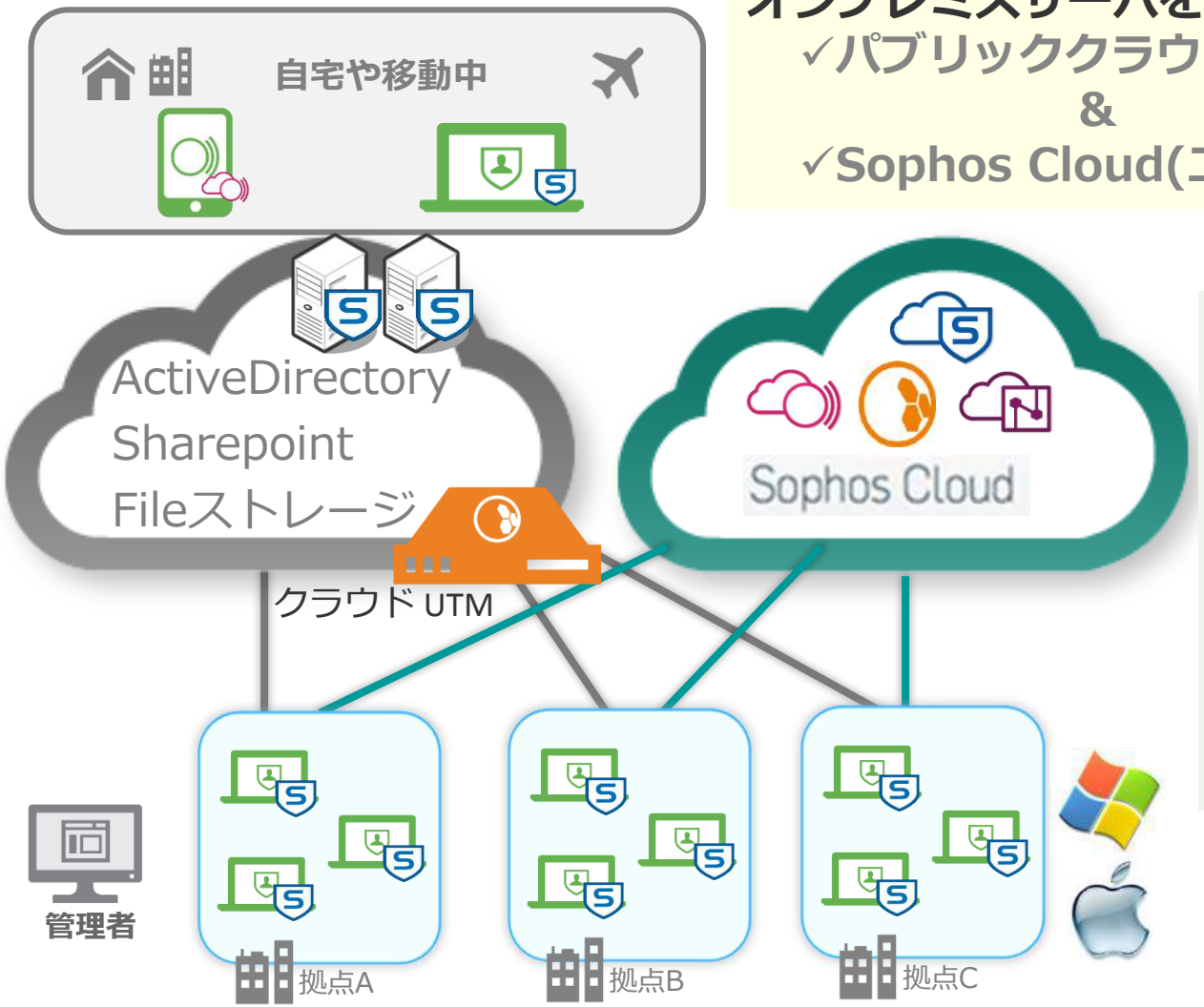
クラウド x クラウド　モデル

オンプレミスサーバを持たない運用に最適

✓パブリッククラウド

&

✓Sophos Cloud(エンドポイント+モバイル)



- ✓ クラウド使用により、サーバーの構築や管理の必要なし
- ✓ インストール直後から、標準のセキュリティポリシーが適用されるので安心・安全
- ✓ インターネットにアクセスできれば、どこからでも展開可能
- ✓ アップデートの管理をする必要がない
- ✓ AWS環境で仮想UTMを利用しVPN、Webフィルタリングを使用

SOPHOS

ライセンス

AWS利用時のライセンス形態

■ ライセンス費用も含めてAWSへ支払う従量課金

- 見積や発注手続きが不要
- 即日から利用可能
- Full-Guardライセンス利用で従量課金

SOPHOS

Free Trial

Sophos UTM 9

★★★★★ (3) | Version 9.105 | Sold by Sophos

$0.10 to $18.40/hr for software + AWS usage fees

plus $175 in AWS Credits Available, learn more at: https://aws.amazon.com/marketplace/cp/SecurityFreeTrial . Sophos UTM 9 (formerly Astaro Security Gateway) is a complete ...

Linux/Unix, Other 9.1 | 64-bit Amazon Machine Image (AMI)

■ 年間ライセンスを一括購入してAWSの環境を利用する（BYOL）

- 特定の機能だけを利用する場合に適切
- ライセンスは持込
- セキュリティアプライアンス製品における標準的なライセンス利用形態

SOPHOS

Sophos UTM 9 BYOL

★★★★★ (3) | Version 9.105 | Sold by Sophos

Bring Your Own License + AWS usage fees

Sophos UTM 9 (formerly Astaro Security Gateway) is a complete security platform that gives all features in a single Amazon Machine Image. For networks from 10-10,000+ users, ...

Linux/Unix, Other 9.1 | 64-bit Amazon Machine Image (AMI)

従量課金ライセンス

1. プロテクションサブスクリプションの選択
(カバーするアドレスならびに期間で価格決定)

- エッセンシャルF/W
- ネットワークプロテクション(有料)
- Web プロテクション (有料)
- メールプロテクション (有料)
- ワイヤレスプロテクション (有料)
- Webサーバプロテクション (有料)

フルガード

2. アドオンの選択
(別売)

- SUM (Free)
- iView (有料)
- RED (有料)
- APs (有料)

3. サポートレベル
の選択

なし
（コミュニティベース）

BYOLライセンス

1. プロテクションサブスクリプションの選択
(カバーするアドレスならびに期間で価格決定)

- エッセンシャルF/W
- ネットワークプロテクション(有料)
- Web プロテクション (有料)
- メールプロテクション (有料)
- ワイヤレスプロテクション (有料)
- Webサーバプロテクション (有料)

フルガード

2. アドオンの選択
(別売)

- SUM (Free)
- iView (有料)
- RED (有料)
- APs (有料)
- エンドポイント (有料)

3. サポートレベルの選択

- UTM スタンダード
- UTMプレミアム

※AutoScaling 利用時は10インスタンスまで同時利用可能

Q&A

SOPHOS