IPSec今昔物語

Shishio Tsuchiya
shtsuchi@arista.com

今昔物語集

- 『**今昔物語集**』（こんじゃくものがたりしゅう）とは平安時代末期に成立したと見られる説話集である。全31巻。ただし8巻・18巻・21巻は欠けている。『今昔物語集』という名前は、各説話の全てが「**今ハ昔**」という書き出しから始まっている事に由来する便宜的な通称である。　https://ja.wikipedia.org/wiki/今昔物語集

Agenda

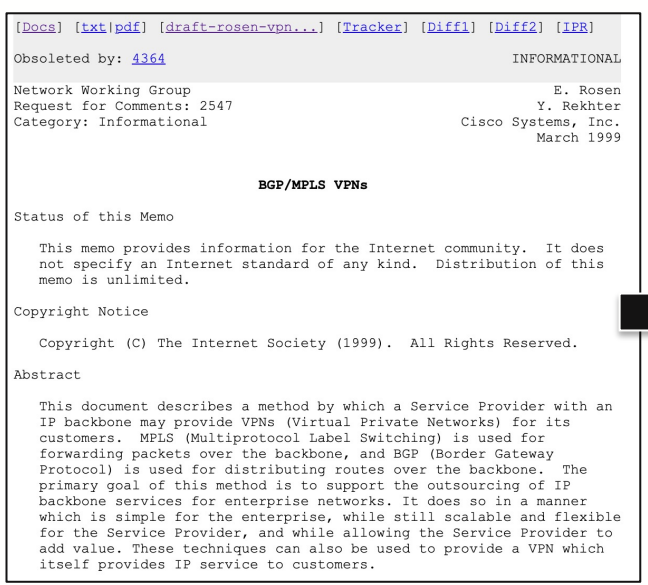
- IPSecの問題点
- 専用線区間での暗号化手法
- これからのIPSec

あなたのデータは他者が見る事出来ますか？

あなたのデータは他者が見る事出来ますか？

RFC2547bis

https://datatracker.ietf.org/doc/html/draft-ietf-l3vpn-rfc2547bis-03



[Docs] [txt|pdf] [draft-rosen-vpn...] [Tracker] [Diff1] [Diff2] [IPR]

Obsoleted by: 4364 INFORMATIONAL

Network Working Group E. Rosen
Request for Comments: 2547 Y. Rekhter
Category: Informational Cisco Systems, Inc.
March 1999

BGP/MPLS VPNs

Status of this Memo

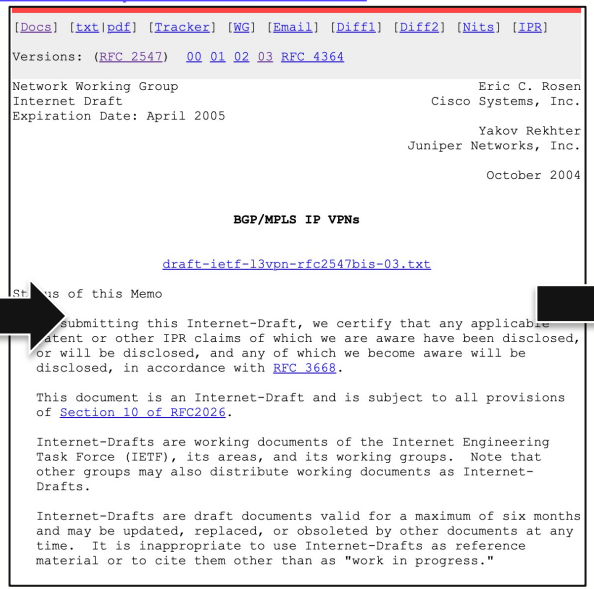
This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1999). All Rights Reserved.

Abstract

This document describes a method by which a Service Provider with an IP backbone may provide VPNs (Virtual Private Networks) for its customers. MPLS (Multiprotocol Label Switching) is used for forwarding packets over the backbone, and BGP (Border Gateway Protocol) is used for distributing routes over the backbone. The primary goal of this method is to support the outsourcing of IP backbone services for enterprise networks. It does so in a manner which is simple for the enterprise, while still scalable and flexible for the Service Provider, and while allowing the Service Provider to add value. These techniques can also be used to provide a VPN which itself provides IP service to customers.



[Docs] [txt|pdf] [Tracker] [WG] [Email] [Diff1] [Diff2] [Nits] [IPR]

Versions: (RFC 2547) 00 01 02 03 RFC 4364

Network Working Group Eric C. Rosen
Internet Draft Cisco Systems, Inc.
Expiration Date: April 2005

Yakov Rekhter
Juniper Networks, Inc.

October 2004

BGP/MPLS IP VPNs

draft-ietf-l3vpn-rfc2547bis-03.txt

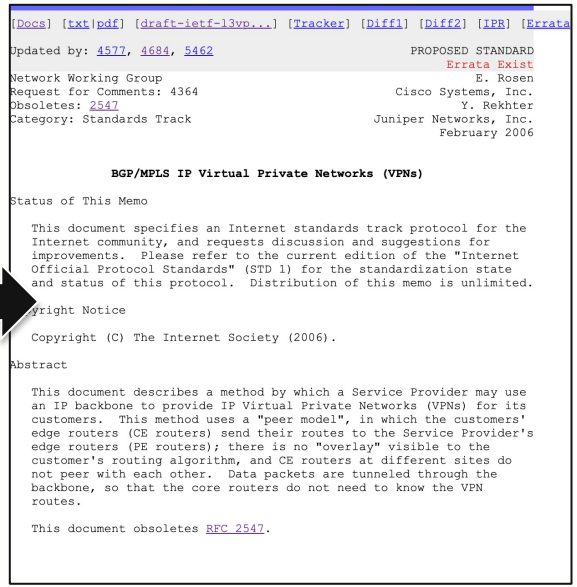
Status of this Memo

By submitting this Internet-Draft, we certify that any applicable patent or other IPR claims of which we are aware have been disclosed, or will be disclosed, and any of which we become aware will be disclosed, in accordance with RFC 3668.

This document is an Internet-Draft and is subject to all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."



[Docs] [txt|pdf] [draft-ietf-l3vp...] [Tracker] [Diff1] [Diff2] [IPR] [Errata

Updated by: 4577, 4684, 5462 PROPOSED STANDARD
Errata Exist

Network Working Group E. Rosen
Request for Comments: 4364 Cisco Systems, Inc.
Obsoletes: 2547 Y. Rekhter
Category: Standards Track Juniper Networks, Inc.
February 2006

BGP/MPLS IP Virtual Private Networks (VPNs)

Status of This Memo

This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This document describes a method by which a Service Provider may use an IP backbone to provide IP Virtual Private Networks (VPNs) for its customers. This method uses a "peer model", in which the customers' edge routers (CE routers) send their routes to the Service Provider's edge routers (PE routers); there is no "overlay" visible to the customer's routing algorithm, and CE routers at different sites do not peer with each other. Data packets are tunneled through the backbone, so that the core routers do not need to know the VPN routes.

This document obsoletes RFC 2547.

- RFC2547でIPベースのネットワークでMPLSを使って、VPNサービスを提供する方法を提示
- その後2547bisを得て、RFC4364で標準化
- bis : twice/again/encore

もう一つのRFC2547bis

https://datatracker.ietf.org/doc/html/draft-ietf-l3vpn-ipsec-2547-05

[Docs] [txt|pdf] [draft-rosen-vpn...] [Tracker] [Diff1] [Diff2] [IPR]

Obsoleted by: 4364 INFORMATIONAL

Network Working Group E. Rosen
Request for Comments: 2547 Y. Rekhter
Category: Informational Cisco Systems, Inc.
March 1999

BGP/MPLS VPNs

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1999). All Rights Reserved.

Abstract

This document describes a method by which a Service Provider with an IP backbone may provide VPNs (Virtual Private Networks) for its customers. MPLS (Multiprotocol Label Switching) is used for forwarding packets over the backbone, and BGP (Border Gateway Protocol) is used for distributing routes over the backbone. The primary goal of this method is to support the outsourcing of IP backbone services for enterprise networks. It does so in a manner which is simple for the enterprise, while still scalable and flexible for the Service Provider, and while allowing the Service Provider to add value. These techniques can also be used to provide a VPN which itself provides IP service to customers.

[Docs] [txt|pdf] [Tracker] [WG] [Email] [Diff1] [Diff2] [Nits]

Versions: 00 01 02 03 04 05

Network Working Group Eric C. Rosen
Internet Draft Cisco Systems, Inc.
Expiration Date: March 2005

Jeremy De Clercq
Olivier Paridaens
Yves T'Joens
Alcatel

Chandru Sargor
Cosine Communications

September 2004

Use of PE-PE IPsec in RFC2547 VPNs

draft-ietf-l3vpn-ipsec-2547-03.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with RFC 3668.

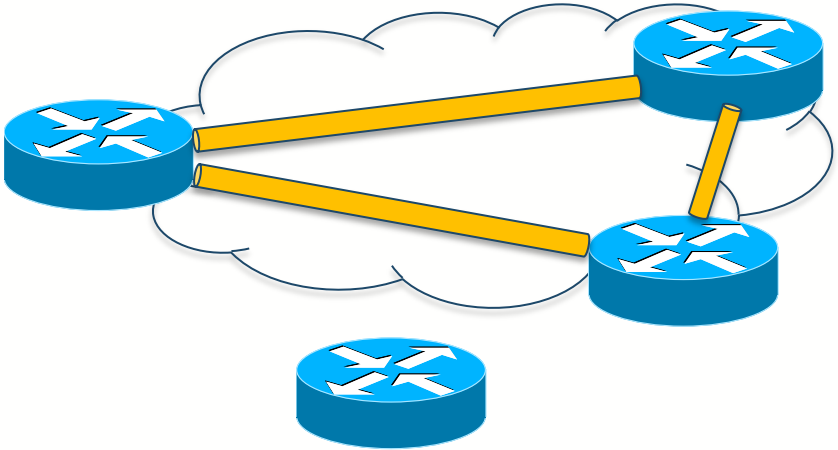
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

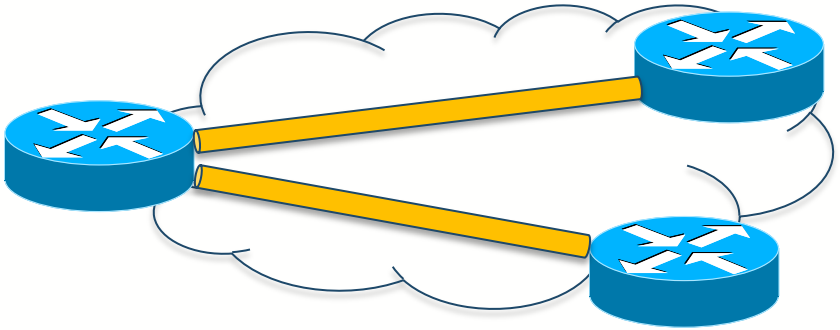
Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

- MPLSで使用するVPNサービスの秘匿性の問題などを解決する一つのオプションとして、PE-PE間でIPSecも併用する事を提案
- ATM/HDLCなどのレイヤー2のサービス以上のセキュリティを担保出来るサービス
- しかし標準化に到達せず

企業側のIPSec VPN

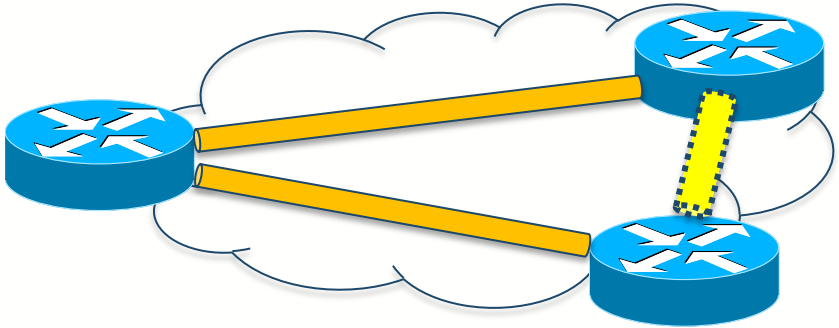




- IPSecを拠点間で結ぶとすべてのノードで同様なIPSecスケーラビリティが必要
- HUB&Spokeでも良いが音声通信など直接やり取りが必要なアプリケーションも想定される
- 追加の拠点が出来た時に全拠点に設定追加が必要

Cisco DMVPN

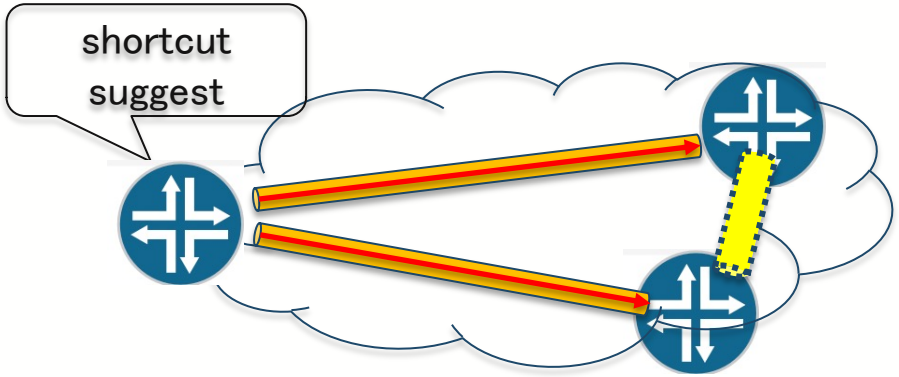
https://tools.ietf.org/html/draft-detienne-dmvpn-01



- NBMA(Non-Broadcast Multiple Access)で使うNHRP(RFC2332)をIPSec環境に流用
- 接続すべき相手をクライアントに指示
- クライアントはその相手にIPSecで接続、通信が終わったらIPSecを終える

Juniper Auto Discovery VPN Protocol

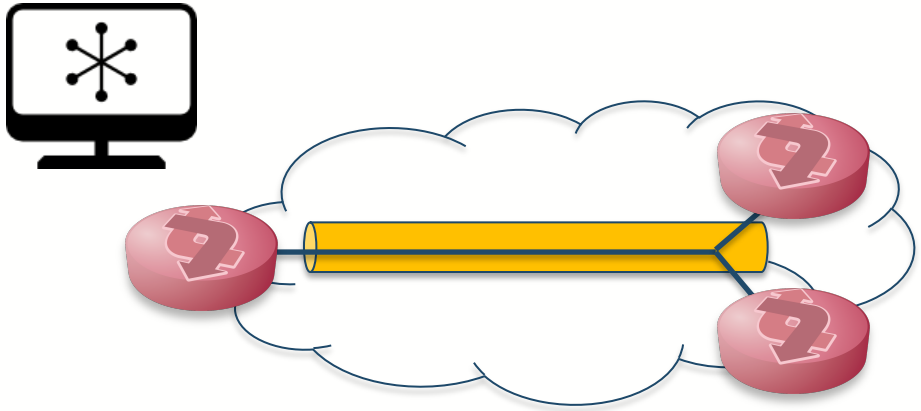
https://tools.ietf.org/html/draft-sathyanarayan-ipsecme-advpn



- ADVPN(Auto Discovery VPN)のサポート可否をネゴシエーション
- サポート可能な場合,Shortcutでの接続を提案する
- ペアは特定期間のみ接続可能なVPNトンネルを確立する

Furukawa Multi-Point SA

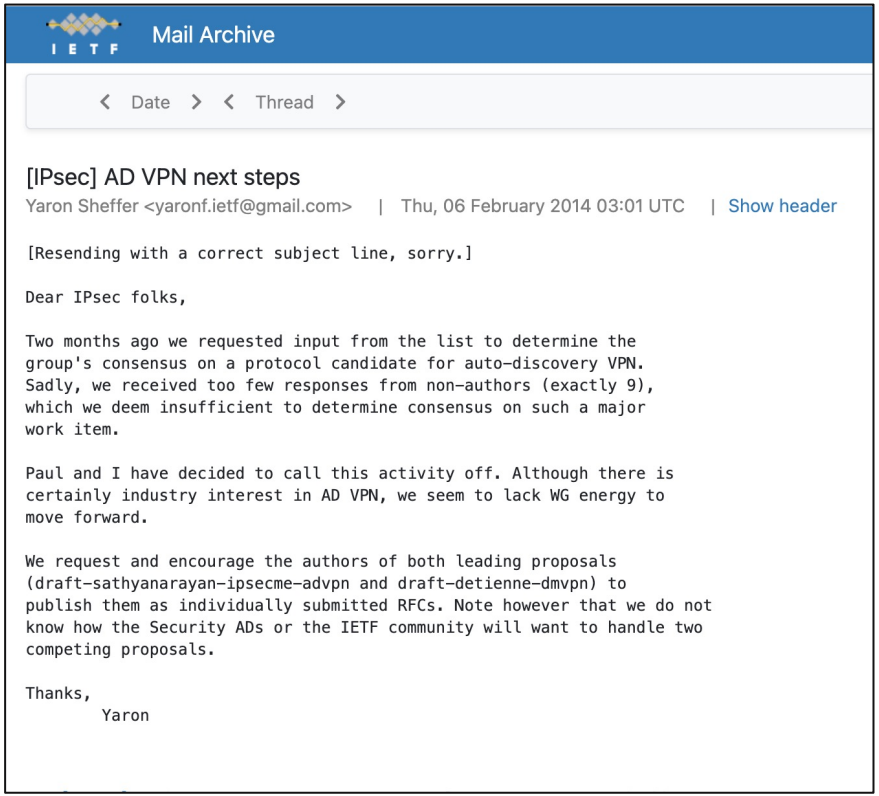
https://tools.ietf.org/html/draft-yamaya-ipsecme-mpsa



- すべてのCPEで共通に使用可能なMulti-Point SAを定義する
- コントローラーがMulti-point SAを作成し、すべてのCPEに配布する

AD VPNの標準化

https://mailarchive.ietf.org/arch/msg/ipsec/sT1CS9s5okz5EmAwpa0tNZPejMU/



Mail Archive

Date Thread

[IPsec] AD VPN next steps

Yaron Sheffer <yaronf.ietf@gmail.com> | Thu, 06 February 2014 03:01 UTC | Show header

[Resending with a correct subject line, sorry.]

Dear IPsec folks,

Two months ago we requested input from the list to determine the group's consensus on a protocol candidate for auto-discovery VPN. Sadly, we received too few responses from non-authors (exactly 9), which we deem insufficient to determine consensus on such a major work item.

Paul and I have decided to call this activity off. Although there is certainly industry interest in AD VPN, we seem to lack WG energy to move forward.

We request and encourage the authors of both leading proposals (draft-sathyanarayan-ipsecme-advpn and draft-detienne-dmvpn) to publish them as individually submitted RFCs. Note however that we do not know how the Security ADs or the IETF community will want to handle two competing proposals.

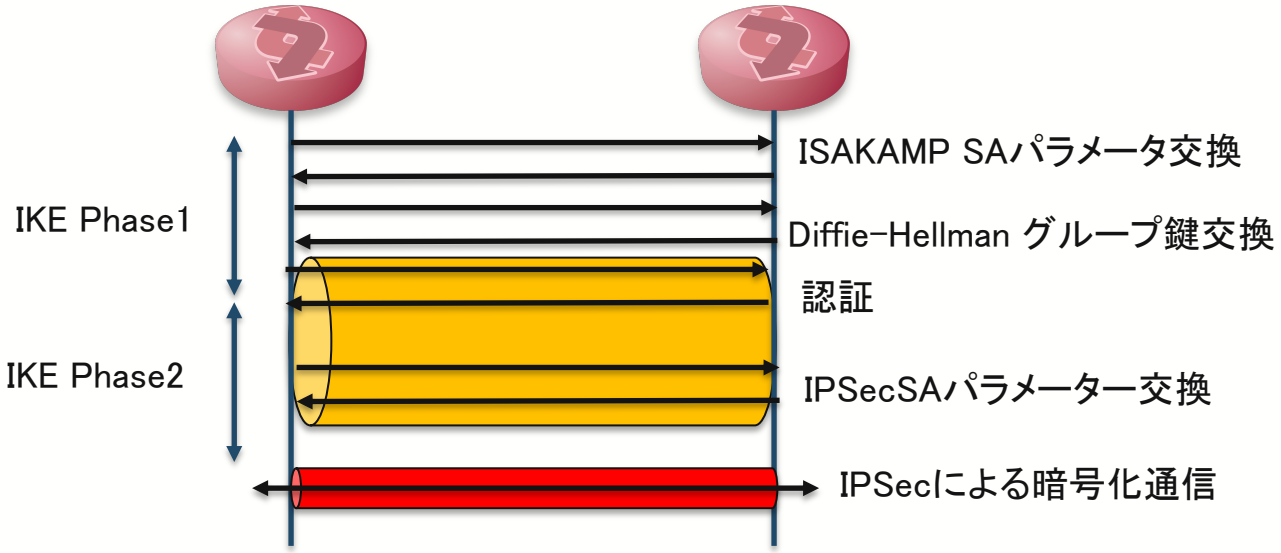
Thanks,
Yaron

- 有力な2つな提案があり、業界としてとても興味にも関わらず、Author以外からの投稿も無く、同意に至らずWGの力が無いとし、標準化活動を停止

IPSec相互接続性

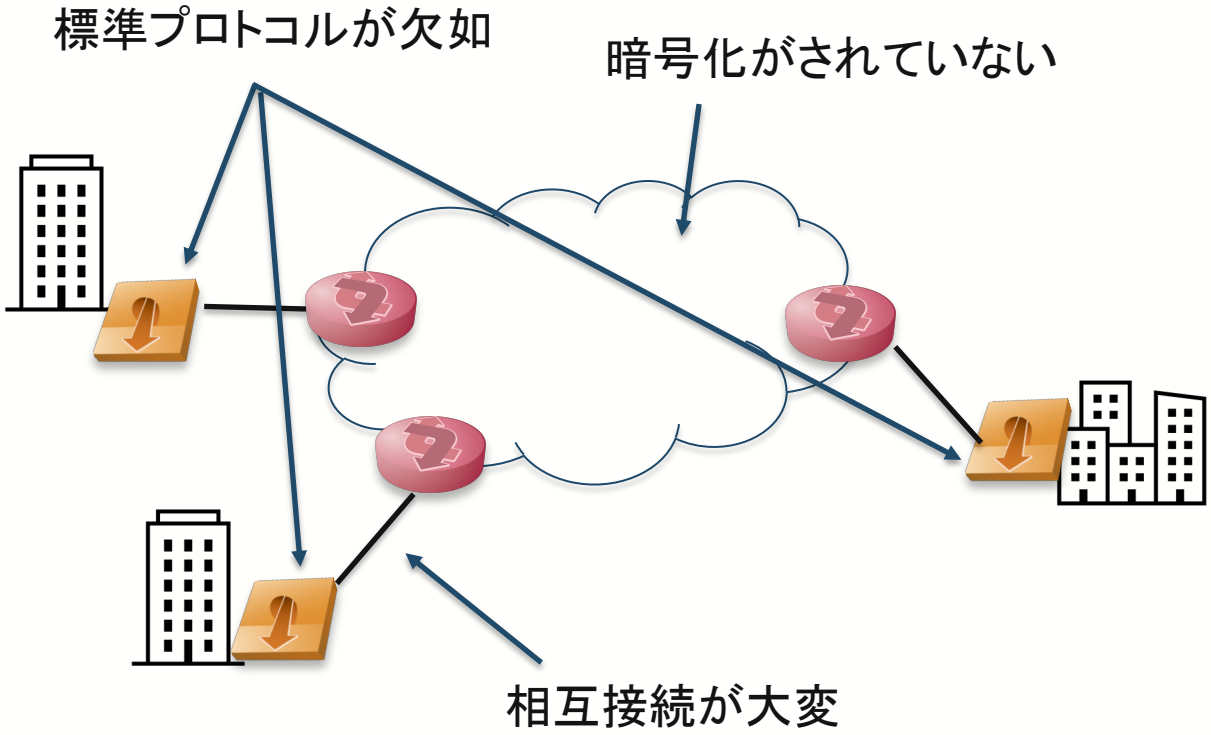
- 現在のVPN機器は異なる機器であっても接続は可能である。しかし、異なる機器間の相互接続を安定稼働させるには、事前に各機器の特徴を確認する必要がある。なぜならば、RFCで標準化されているIPSecプロトコルにはあいまいな記述が多く、その部分の実装が機器により異なるためである。
  - **異機種間のIPSecVPN構築の注意点** https://www.atmarkit.co.jp/ait/articles/0312/13/news003.html
- 製品個々の設定に「ノウハウ」と呼べるようなパラメータ設定の「癖」が存在する。今回の実証実 験ではこれらを大きくまとめようと試みたが、現状の製品群では結局個々の製品設定の特性として意識せざるを得ない結果となった。
  - **電子政府情報セキュリティ技術開発事業 IPsec相互接続に関する調査** https://www.jnsa.org/active/houkoku/main-matome.pdf

IPSecシーケンス



- 手順が複雑で定義が曖昧の為相互接続が取りにくい
- ISAKAMP SAとIPSecSA2つのライフタイムがあり、これを更新するタイミング(Re-Key)も注意が必要
- 既に暗号化されている事もあり、トラブルシューティングが容易では無い

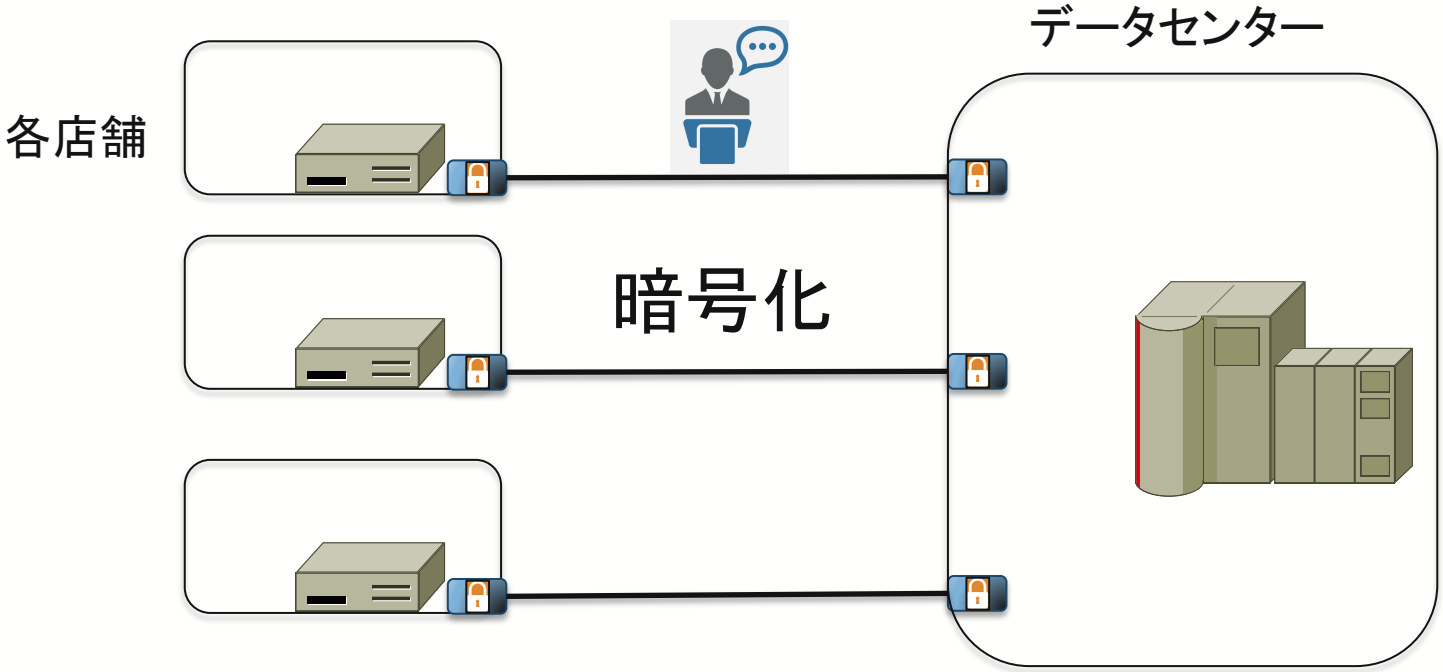
IPSecの問題点



Agenda

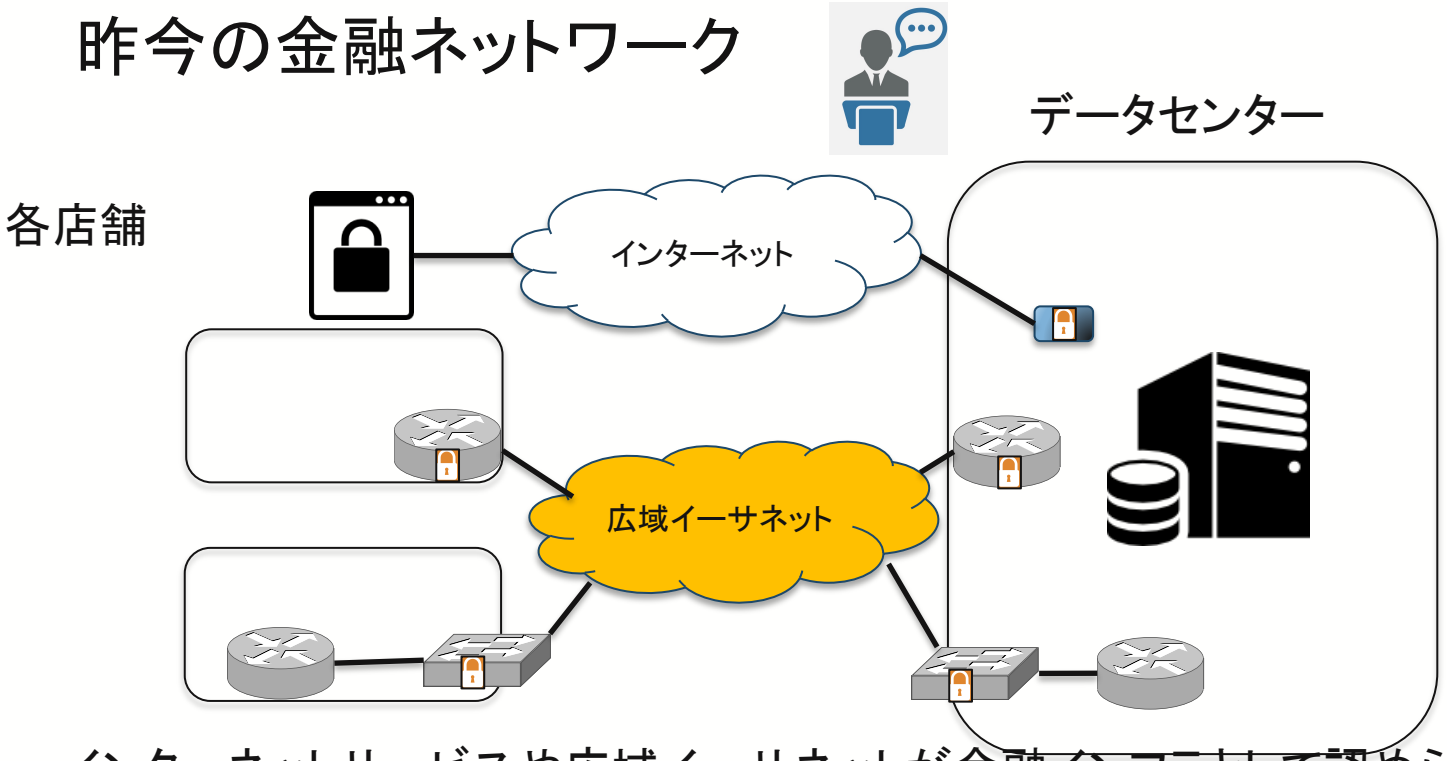
- IPSecの問題点
- 専用線区間での暗号化手法
- これからのIPSec

昔の金融ネットワーク



- T1回線などの間に暗号化装置を入れて、キャリアであったとしても通信を見る事が出来ない

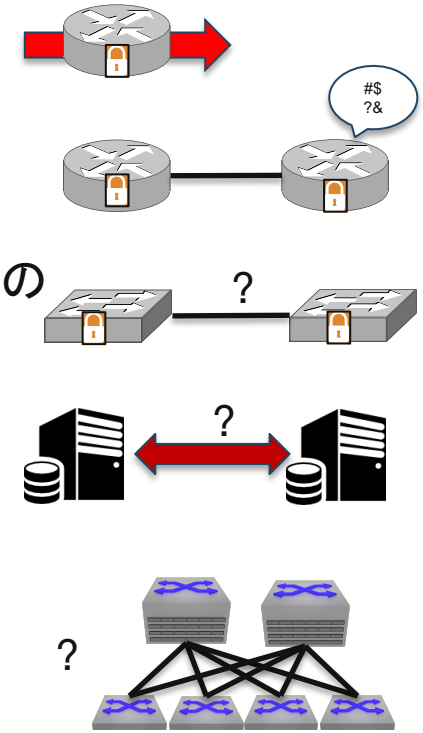
昨今の金融ネットワーク



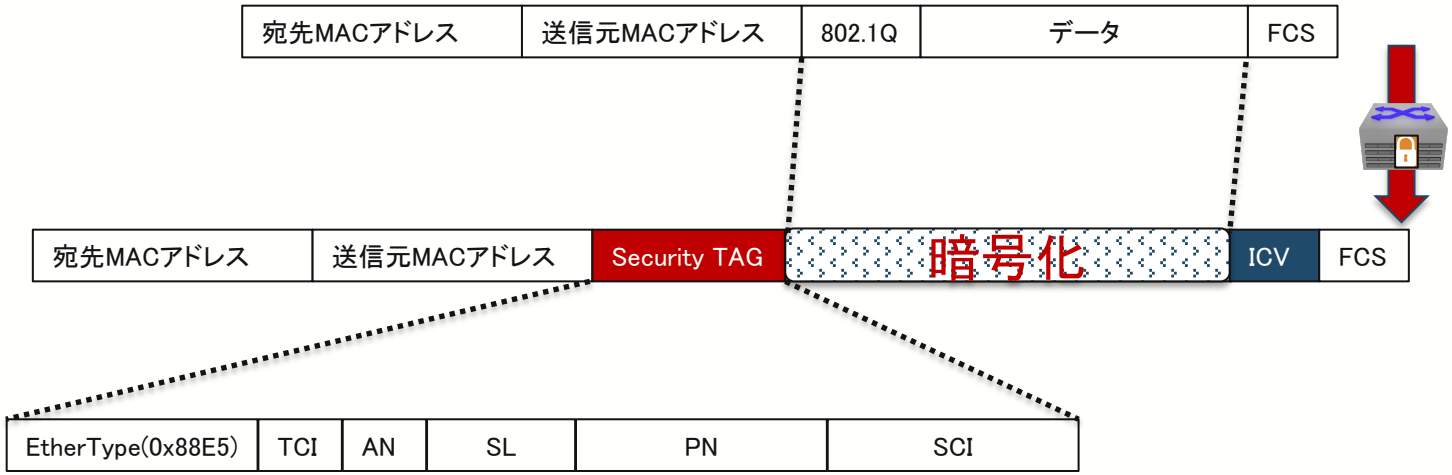
- インターネットサービスや広域イーサネットが金融インフラとして認められ、様々な暗号化プロトコルが使用されるようになった
- SSL インターネット
- IPSec /独自イーサネット暗号化スイッチ

昨今の金融ネットワークでの暗号化の考慮点

- IPSecルータのパフォーマンス
- IPSecルータの異機種間での相互接続性:IKEv2?
- イーサネット・スイッチでの暗号化手法
- ディザスターリカバリーなど信頼性を高める為のDCIでの暗号化手法
- クラウド型データセンターでの暗号化方式
  - スケール型のネットワークでどのように暗号化を提供するか?
- プライベートクラウドでの展開

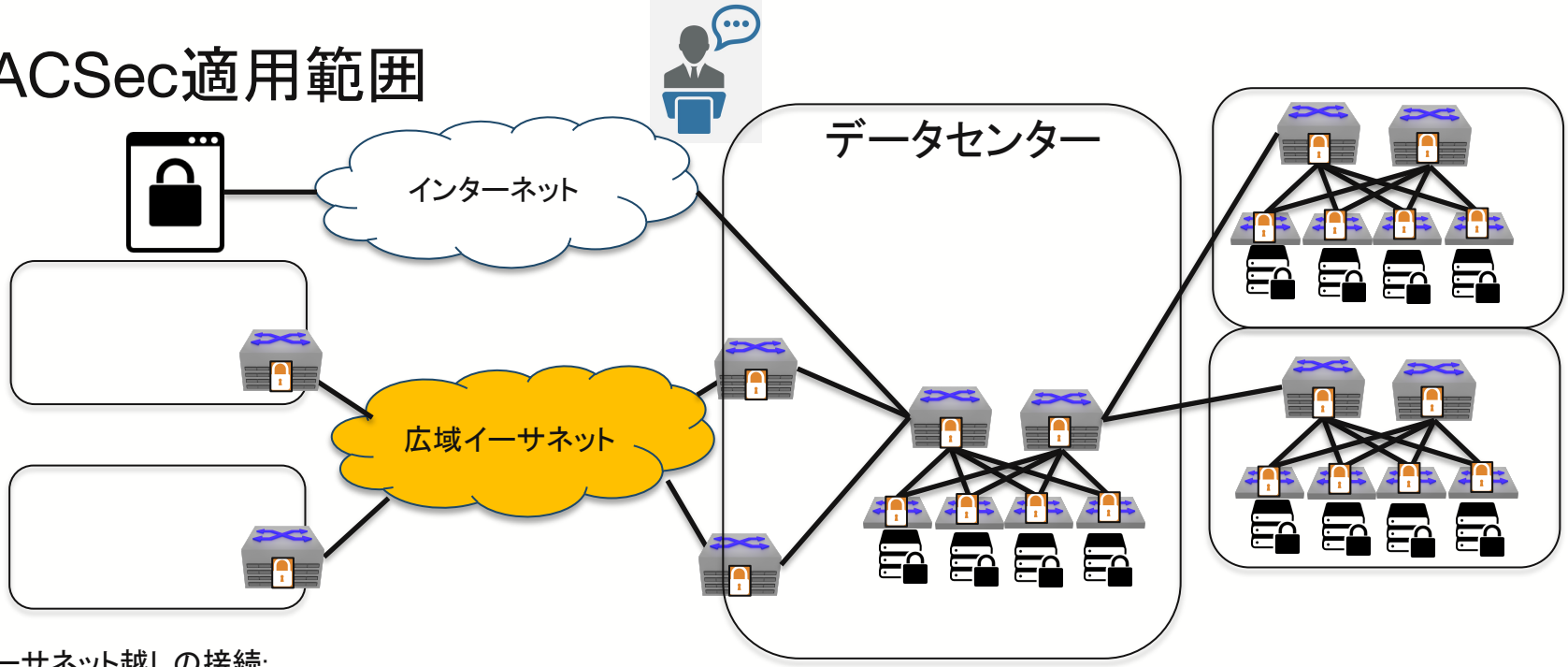


IEEE802.1AE(Mac Security)



- 2006年に標準化された方式: 2011年 802.1AEbn/2013年802.1AEbwと拡張
- IEEE802.1AE(MACSec)ではオリジナルフレームの802.1q情報以下のデータは全て暗号化される
- Security TAGおよびICV(Message Authentication Code)が付与される

MACSec適用範囲



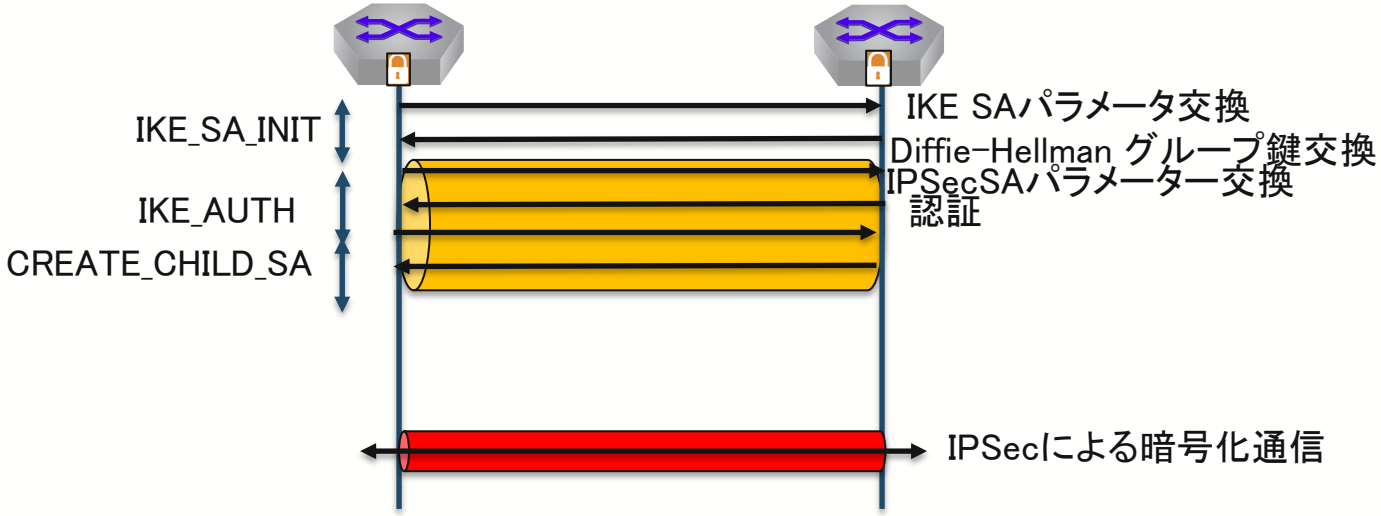
- 広域イーサネット越しの接続:
  - IPSec相互接続問題やパフォーマンス問題を解消
  - 独自暗号化設備からの解放
- データセンター内
  - スケール型ネットワークデザインでアプリケーションレイヤーのみならずインフラでも暗号化
- データセンター間
  - パフォーマンス劣化/相互接続問題無しでセキュアな接続

Agenda

- IPSecの問題点
- 専用線区間での暗号化手法
- これからのIPSec

IKEv2 RFC7296

https://datatracker.ietf.org/doc/html/rfc7296



- メッセージを簡潔に明確に

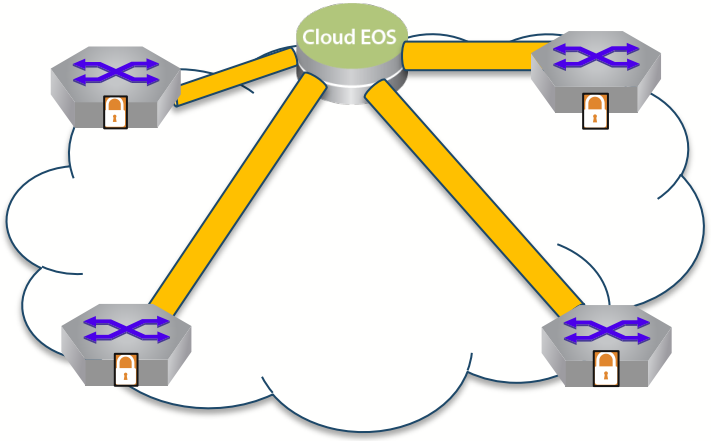
Strong Swan

https://www.strongswan.org/

- オープンソースのIPSec実装
  - IKEデーモン
  - Linux 2.6, 3.x 4.x カーネル,Android,FreeBSD,OS X,iOS ,Windows
  - IKEv1/IKEv2サポート
- 相互接続性
  - https://wiki.strongswan.org/projects/strongswan/wiki/Interoperability
  - Windows 7以降 IKEv2
  - Windows Suite B サポート　IKEv1
  - Apple iOS (iPhone, iPad) と Mac OS X　IKEv1/IKEv2
  - strongSwan 4.x (pluto) - 5.x (charon)　IKEv1
  - Blackberry OS 10　IKEv2
  - CISCO
  - Fortinet
  - Check Point
  - Juniper
- Cloudプラットフォームでの使用
  - Kernelやユーザースペースはそのままで良い為、比較的簡単
  - 一般的に、クラウド環境では、基盤となるネットワークが、送信されたIPパケットのソースIPアドレスをチェックする
  - AWS/Azureではこれを無効化するオプションがある

Secure EVPN

https://tools.ietf.org/html/draft-sajassi-bess-secure-evpn




```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       MAC Header              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Eth Type = IPv4/IPv6          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     IP Header                 |
|     Protocol = UDP            |
+-------------------------------+
|       UDP Header              |
| Dest Port = VxLAN             |
+-------------------------------+
|      VxLAN Header             |
+-------------------------------+
|     Inner MAC Header          |
+-------------------------------+
|     Inner Eth Payload         |
+-------------------------------+
|         CRC                   |
+-------------------------------+
```

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       MAC Header              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Eth Type = IPv4/IPv6          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     IP Header                 |
|     Protocol = ESP            |
+-------------------------------+
|     ESP Header                |
+-------------------------------+
|       UDP Header              |
| Dest Port = VxLAN             |
+-------------------------------+
|     VxLAN Header              |
+-------------------------------+
|     Inner MAC Header          |
+-------------------------------+
|     Inner Eth Payload         |
+-------------------------------+
|   ESP Trailer (NP=UDP)        |
+-------------------------------+
|         CRC                   |
+-------------------------------+
```

- コントローラー(RR)を使って、直接のIKEv2ピアリングなどはせずにIPSec SAを交換する方法
- VXLANなどのパケットをESPで暗号化
- BGP TunnelアトリビュートをESP-TransportとESP-in-UDP-Transportに対応させる
- MACsecフレームを使う事も可能

14.4 Tb/s StrataDNX™ Jericho2c+ Ethernet Switch Series

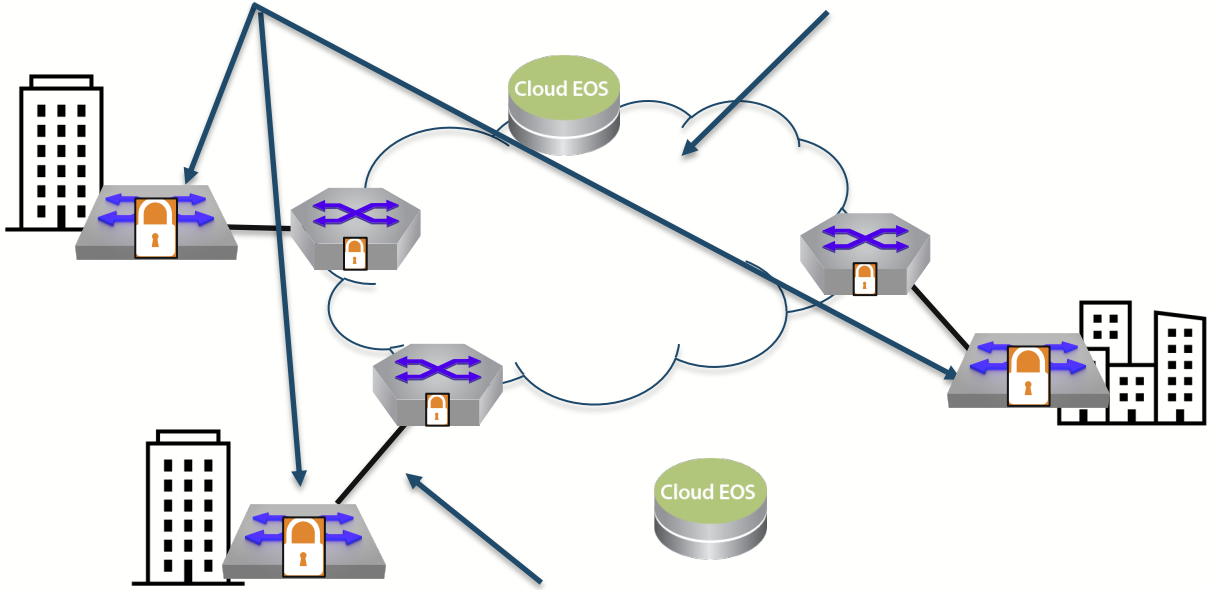
https://jp.broadcom.com/products/ethernet-connectivity/switching/stratadnx/bcm88850

- IPSec/MACSecをラインレートですべてのポートサポート

これからのIPSec

L2/L3すべて暗号化が可能
SecureEVPN/MACSec/VXLAN+IPSec

L2/L3すべて暗号化が可能
SecureEVPN/MACSec/VXLAN+IPSec



IKEv2での相互接続性

ARISTA

まとめ

- IPSecの過去の実装と今をまとめてみた
- かっては相互接続性やパフォーマンスやスケーラビリティに問題があったIPSecもIKEv2による簡素化やコントローラーベースのソリューション、商用シリコンへの実装が行われている

聞きたい事

- ベンダー間のIPSec相互接続を実施してる?
  - IKEv1 or IKEv2?
- L2暗号化をやってる人(言えるのかしら？)
  - IPSec over EoMPLS over GRE?
  - IPSec over L2TPv3?
  - 暗号化装置？
- ADVPN使ってる人?その方式
- 相互接続してる？