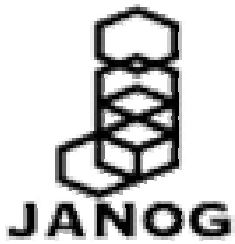


JANOG Interdomain Routing Security Workshop

現状、動向、今後

7 July 2004

河野 美也 Miya Kohno (mkohno@cisco.com)

Agenda

- **現状**
  - 2004年5月26日 Security Workshop (@SanJose)から
- **動向**
  - Control Plane
  - Forwarding Plane
  - Management Plane
- **今後**
  - 今後の方向性

Agenda

- ***現状***
  - 2004年5月26日 Security Workshop (@SanJose)から
- **動向**
  - Control Plane
  - Forwarding Plane
  - Management Plane
- **今後**
  - 今後の方向性

Security Workshop @ SanJose (26 May 2004)

- NANOG31(@SF)開催週、米主要オペレータの方にCisco SanJose本社に立ち寄って戴き、講演戴きました。

- ご講演戴いた方
  - Tim Battle (AT&T Security Operations)
  - Jared Mauch (Verio/NTT Operations)
  - Ryan McDowell (Sprint Operations)
  - Christopher L. Morrow (MCI Security Operations)

- Cisco側参加者
  - **開発エンジニア**
  - **その他エンジニア**

AT&T – 現状

- Receive ACL
  - for GRP protection
- WRED
  - for preventing buffer over utilization
- uRPF + ACL
  - for source address assurance
- Netflow
  - for monitoring and detecting NW anomalies --- getting very important
- Remote Triggered Blackholes
  - for diverting traffic to null0 and scrubbling device
- Configuration auditing
  - for preventing mis-configuration
- Command Automation
  - for quick trouble shooting

AT&T – 要望

- Consistency of configurations and commands across platforms. Feature commands should be identical between platforms and images.

- Consistency of services across SP platform (Netflow, rACLs)

Sprint – Issues

- Lack of MIB for uRPF drops
- Lack of MIB for rACL matches
- Lack of uniform feature support across platforms
  - uRPF, rACL, source-tracker
- Inability to kill “listening” processes
  - e.g. UDP/496 (PIM-RP-DISC)
- ACLs are pathetic
  - Need a bit mask to filter on any bit(s) anywhere in an IP packet
- BGP reorganization
  - Too many CLIs
- BGP route analysis
  - Only way to get full view is screen scrape

Sprint – Issues

- BGP max-prefix
  - Needs to try and reestablish or just stop accepting routes above limit
- No easy way to see how many routes advertised to BGP peer
  - Put advertised routes in “show ip bgp summary”
- “show ip bgp <domain-name>” broken
- uRPF “any route” needed
  - Not just strict mode…
- Source-Tracker
  - Automatic shutoff if pps rate exeeds threshold
  - Only show counts that match an ACL (e.g. TCP/80/SYN)
- Netflow
  - Show cache that maches src/dst address, etc.
- SSH host keys n routers
  - Need a way to copy to new RP

NTT/Verio - Challenges

- Not consistent or implemented on all IOS devices
- Interface ACLs don’t scale
- No way to globally apply acl to all interfaces to block “worm” traffic (e.g. ms-sql/slammer)
- uRPF setting global on 6k
- Lack of consistent packet inspection techniques in router configuration

NTT/Verio - Challenges

- How to stop (filter, police, otherwise) attacks rapidly ?
- Rapidly pushing out configuration changes to hundreds of devices
  - Differences in configuration semantics create troubles and inconsistency (platform, sw rev)
  - Avoiding configuration “drift”
  - Signaling across existing “database” infrastructure via BGP ?

MCI – 要望

- Line Rate ACLs on all interfaces
  - ACLs on all interfaces on all platforms
  - Full packet match capability
- Line Rate ACLs on all platforms (core)
  - Don’t limit acls to edge platforms, todays core is tomorrows edge
- TTL filtering in ACLs and Services
  - Set outbaound ttl/default-ttl

What’s important

- **Consistency, Consistency, Consistency !!**

- **Scalability**
- **Simplicity**
- **Stability**

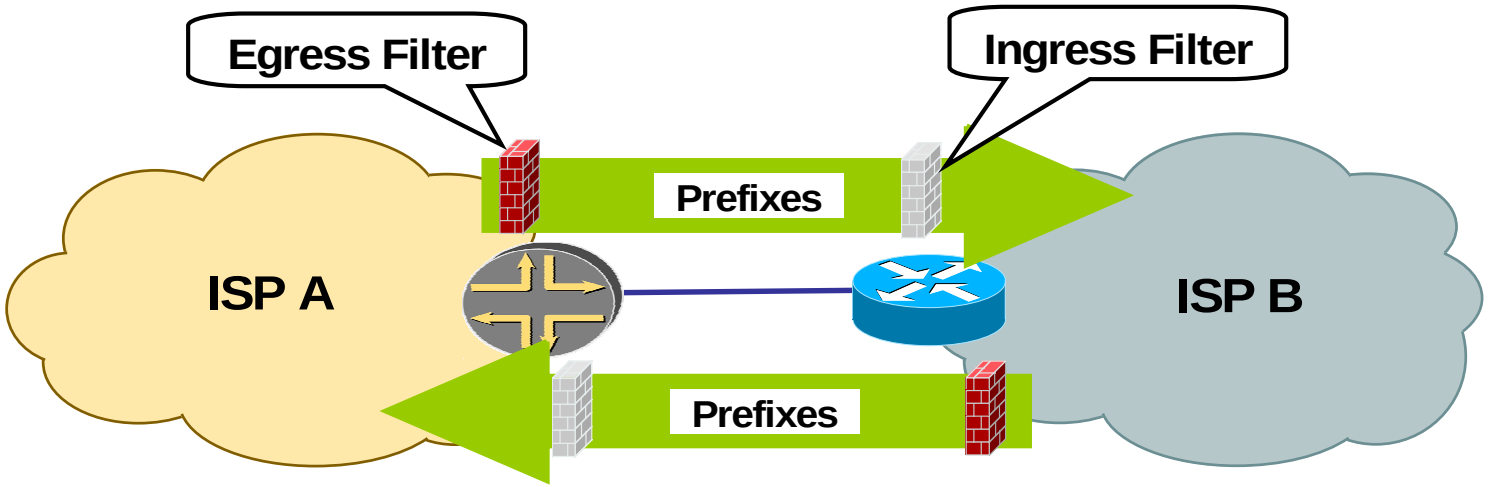
Agenda

- **現状**
  - 2004年5月26日 Security Workshop (@SanJose)から
- ***動向***
  - Control Plane
  - Forwarding Plane
  - Management Plane
- **今後**
  - 今後の方向性

Control Plane

- Control Planeの保護
  - Peering Relationshipをいかに高信頼化するか。
    - Guarded Trust
    - TCP MD5
    - BGP over Ipsec (?!)
    - BTSH/GTSM (RFC3682)
  - 受け取ったprefixが正しいASからoriginateされたものか。
    - S-BGP, SO-BGP (?!!!!)

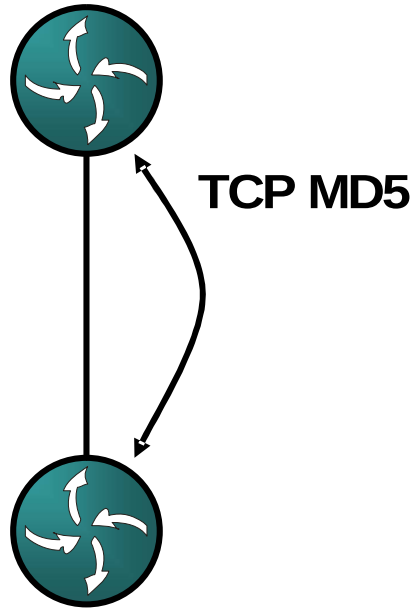
Guarded Trust



- Guarded Trust, Mutual Suspicion (**J**)
- ISP AはISP BがGlobal Internet TableからX prefixesを送ることを信用する。
- ISP Bは、ISP Aに対し、X prefixesのみを送るべく、egress filterを作成する。
- ISP Aは、ISP BがX prefixesのみしか送らないように、igress filterを作成する。
- ISP Aのingress filterは、ISP Bのegress filterを強化する。

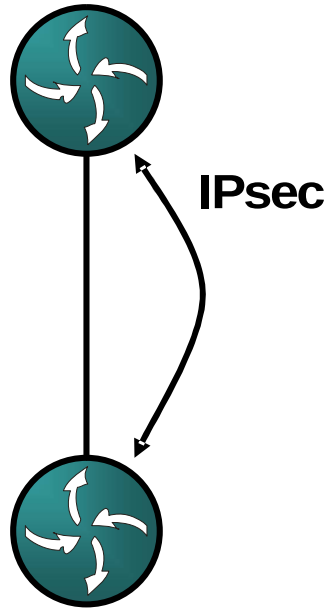
TCP MD5

- **TCP MD5を利用して、パケットのAuthenticationを行なう。**
- **Key distributionはマニュアルで。**
- **RFC1321 ー MD5.**
- **RFC2385 ー MD5 with BGP**
- **RFC3562 ー MD5 keyの構築･管理方法について**



BGP over IPSec

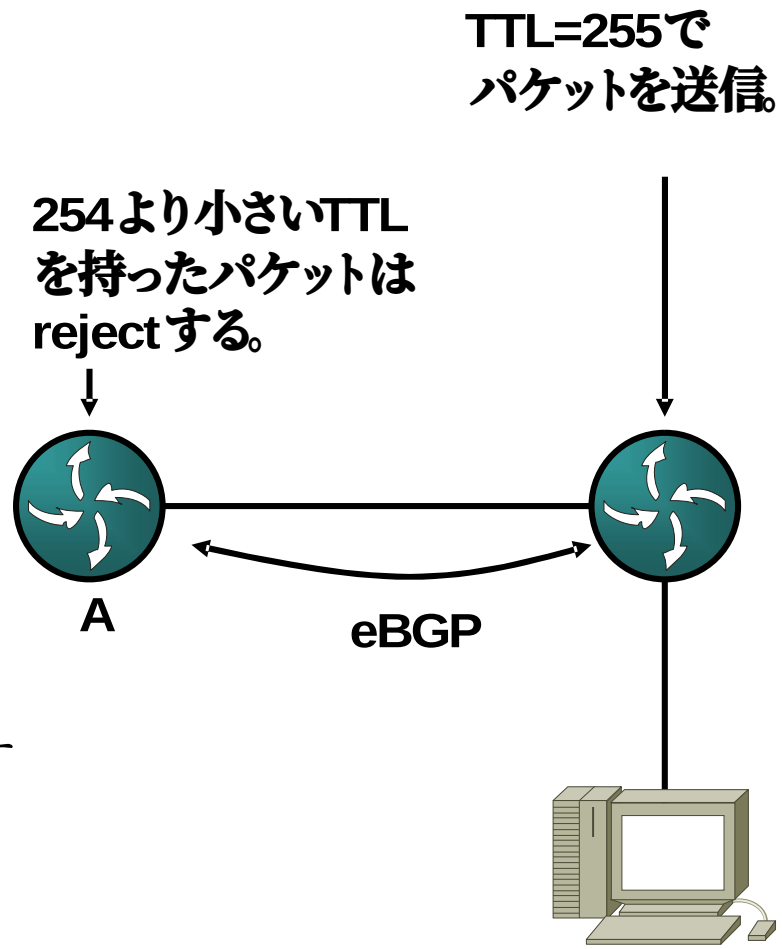
- **IP secをTransportとして使用することにより、Peering Relationのみならず、伝達される情報の中身まで保護することができる。**
- **draft-ward-bgp-ipsec**
- **本当に必要 ?!!!**



TTL sanity check

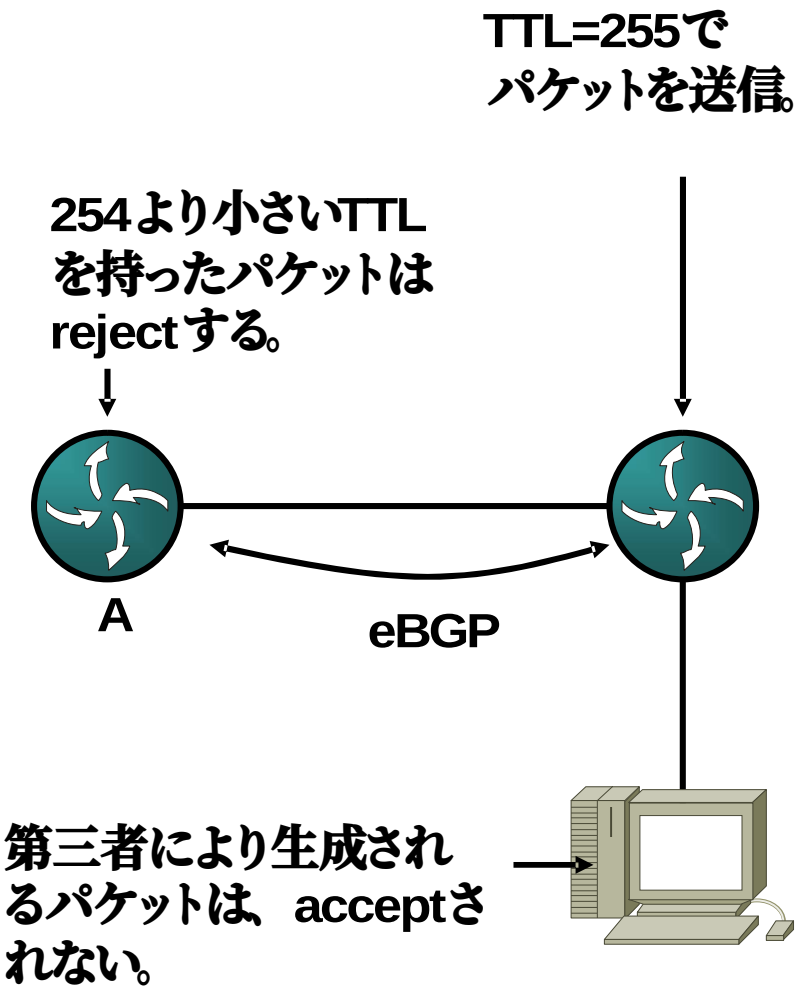
- **BTSH**
  - **BGP TTL security hack**
  - **draft-gill-btsh**
- **GTSM**
  - **Generalized TTL security Mechanism**
  - **RFC3682**

- eBGP speakerは、TTLを最大(=255)にしてパケットを送信する。
- eBGP speakerは、254(とか253とか)よりも低いTTLを持つパケットを受信することを拒否する。



TTL sanity check

- 直接接続されていないdeviceから送信されるパケットは、これらのBGP speakerにはacceptされない。
- BGP speaker同士で合意の上設定する必要がある。



Forwarding Plane

- ACL
  - with performance and scalability
- uRPF
  - Strict
  - Loose (triggered black hole filteringのための基礎)
- Netflow
  - Trafficの傾向分析
  - 異常状態の検出、分析

Management Plane

- Default Access Denied
  - 使用しないプロトコルは落としておく
- AAA & encryption protocols for console login
  - SSH, SSL, IPSec
- Isolation of Management Ports

Agenda

- **現状**
  - 2004年5月26日 Security Workshop (@SanJose)から
- **動向**
  - Control Plane
  - Forwarding Plane
  - Management Plane
- ***今後***
  - 今後の方向性

今後

- まずは、今出来ていないこと、やるべきことをやる。
- What's Next ? ? ?!
  - BGP over IPSec ?!
  - S-BGP / SO-BGP ?
  - Ptomaine
    - Prefix Taxonomy Ongoing Measurement & Internetwork Experiment

    http://www.ietf.org/html.charters/ptomaine-charter.html
  - RPSEC
    - Routing Protocol Security Requirements Working Group

    http://www.ietf.org/html.charters/rpsec-charter.html

S-BGP/SO-BGP

- **現在できること**
  - ルータ自体の保護
  - Peering Relationshipの保護
  - 不必要なルーティング情報のフィルタリング
  - route flapsやexcessive routesからの保護

- **さらなる（違う観点の）セキュリティが必要？**
  - そのASが、そのprefixをoriginateすることは、authorizeされているのか？
  - 広報されたprefixが、実際にoriginateしたAS内で、本当にreachableか？
  - あるprefixを広報しているpeerが、その宛先に対し、少なくとも一つの正当なパスを持っているか？

→ S-BGP, SO-BGP ?!!

S-BGP: http://www.net-tch.bbn.com/sbgp/sbgp-index.html
SO-BGP: ftp://ftp-eng.cisco.com/sobgp/index.html

SO-BGP

- S-BGPはちょっと非現実的では…？

- SO-BGPの考え方
  - いかなる種類のcentral authorityには依存しない。
  - 順次deploy可能でなくてはならない。（全てのASが参加しなくても、ある程度のセキュリティレヴェルを達成する。）
  - deploymentに関する柔軟性を許容しなくてはならない。
  - セキュリティ情報を提供するシグナリング機構は、できるだけ柔軟である必要がある。
  - 現在のBGP実装へのインパクトは最小化すべき。
  - ルーティングを保護するために、ルーティングに頼るべきではない。（外部ルーティングデータベースへの依存？）
  - UPDATEとセキュリティ情報伝播方法の切り離し

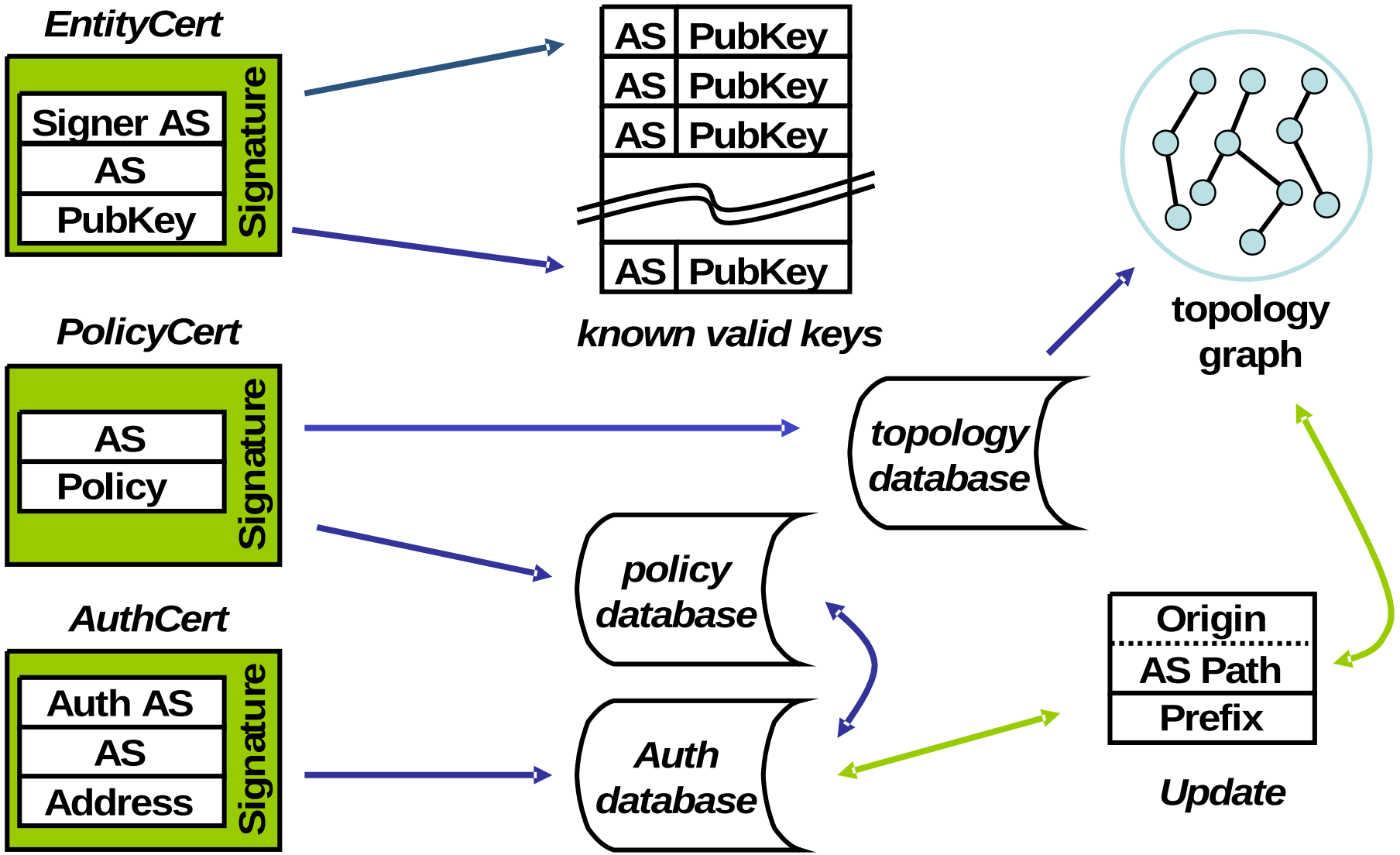
SO-BGPのオペレーション

- Certificate Transport
- Certificate Processing
- Update Processing

Certificate Transport

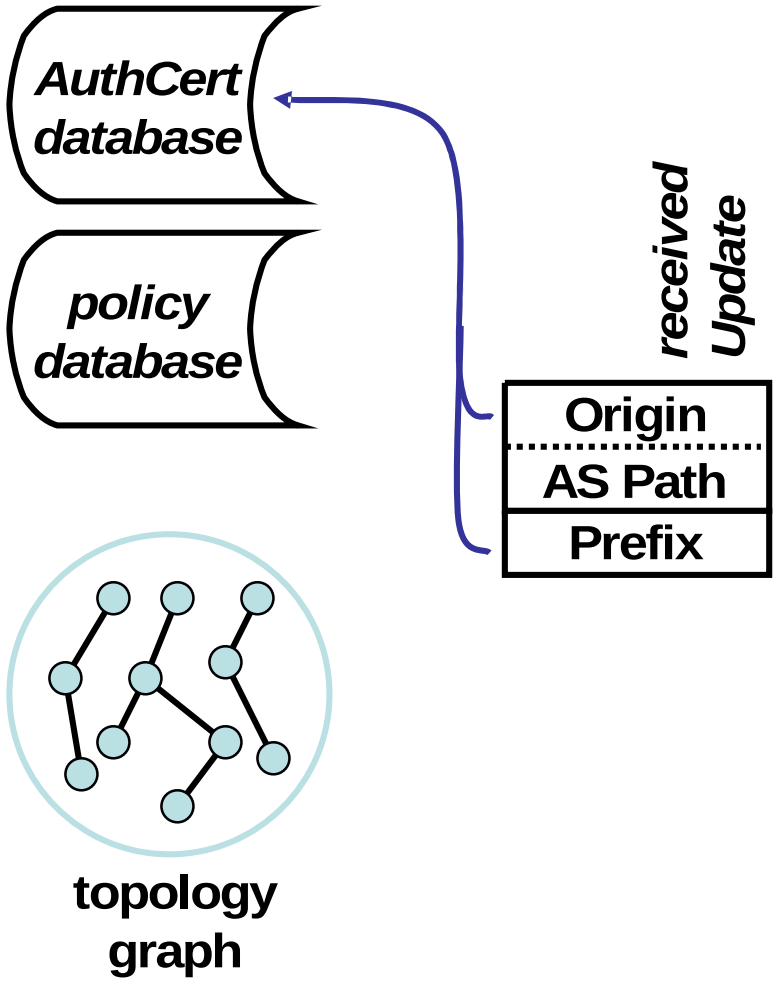
- SO-BGPは、Transport非依存。
- どのようにCertificateがSO-BGPを実行しているdeviceに到達されるかは、基本的にはスコープ外。
- 一つの例として draft-ng-sobgp-bgpextensions
  - New BGP SECURITY message
  - Certificates are carried within TLVs
  - 他の security 関連情報にも応用可能

Certificate Operation



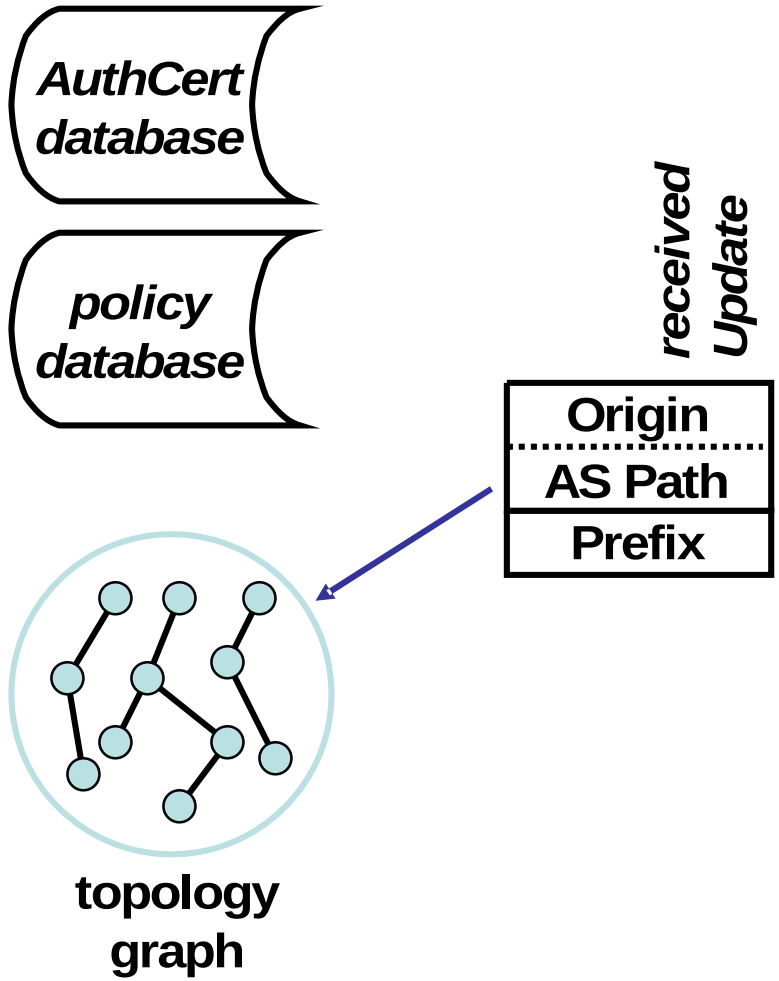
Update Processing

- AS pathの最初のhop(the origin AS) がAuthCertデータベースと照合される。Prefixは、このASが生成することをauthorizeされているレンジ内にある必要がある。
- AuthCertデータベースのエントリーに関連付けられているポリシーチェックが行なわれ、必要なアクションが取られる。



Update Processing

- 次に、AS pathが、既に作成されたトポロジーグラフと照合される。
- AS pathが不正の場合、その経路は廃棄される。

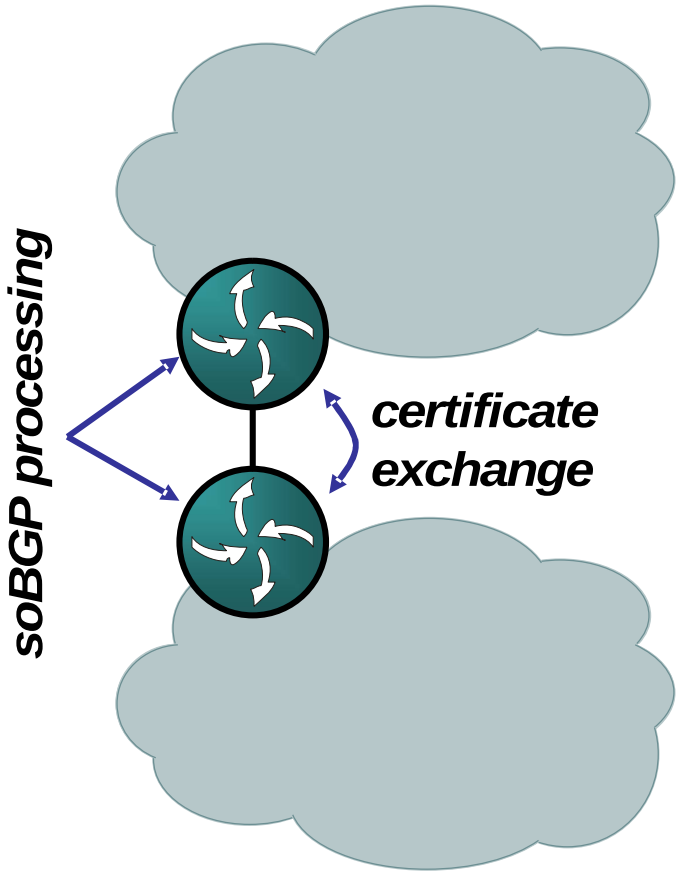


SO-BGP Deployment 考慮点

- Deployment Options
- Incremental Deployment

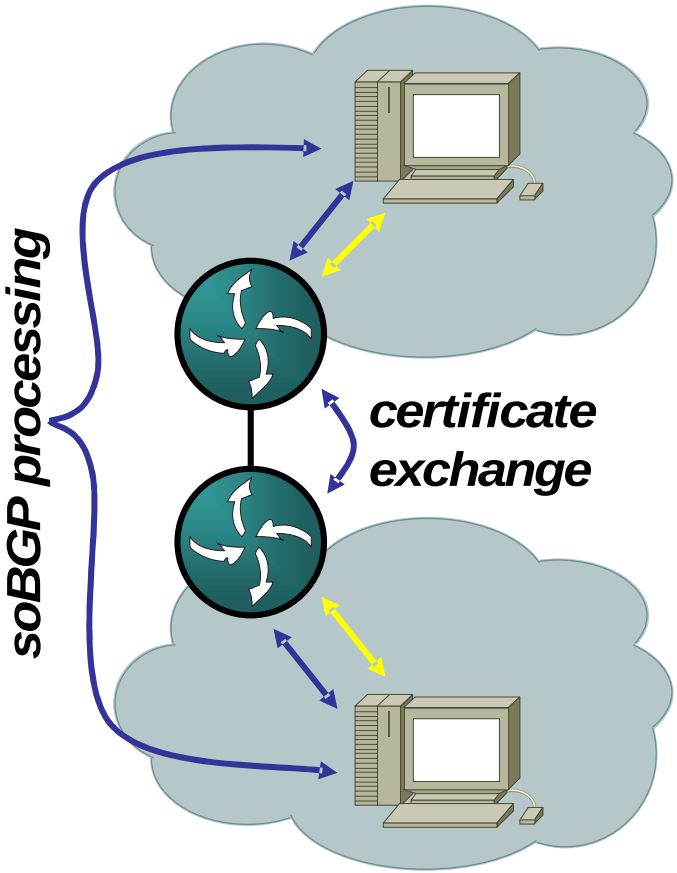
Deployment Options

- eBGP peering point(AS境界) にてcertificateの交換をする。
- 各eBGPスピーカーがcertificateの処理をするための暗号プロセスを走らせる必要がある。



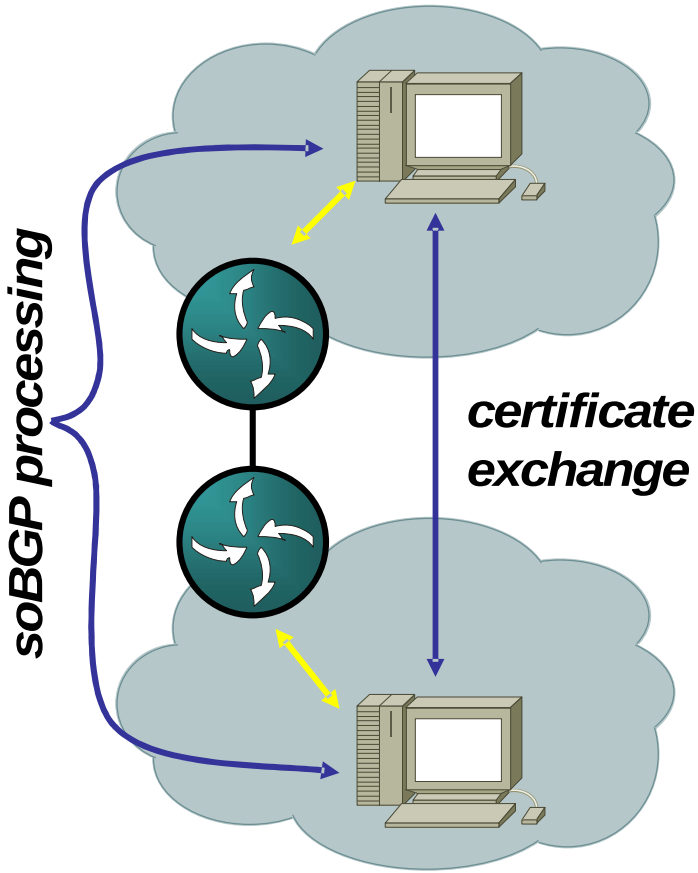
Deployment Options

- iBGPを利用し、AS内のサーバーにcertificate処理をオフロードすることも可能。
- この場合、サーバがcertificate処理、および各種データベースの構築を行なう。
- Edgeルータは、RADIUS等を使用し、サーバを照会してUPDATEをvalidationを行なう。



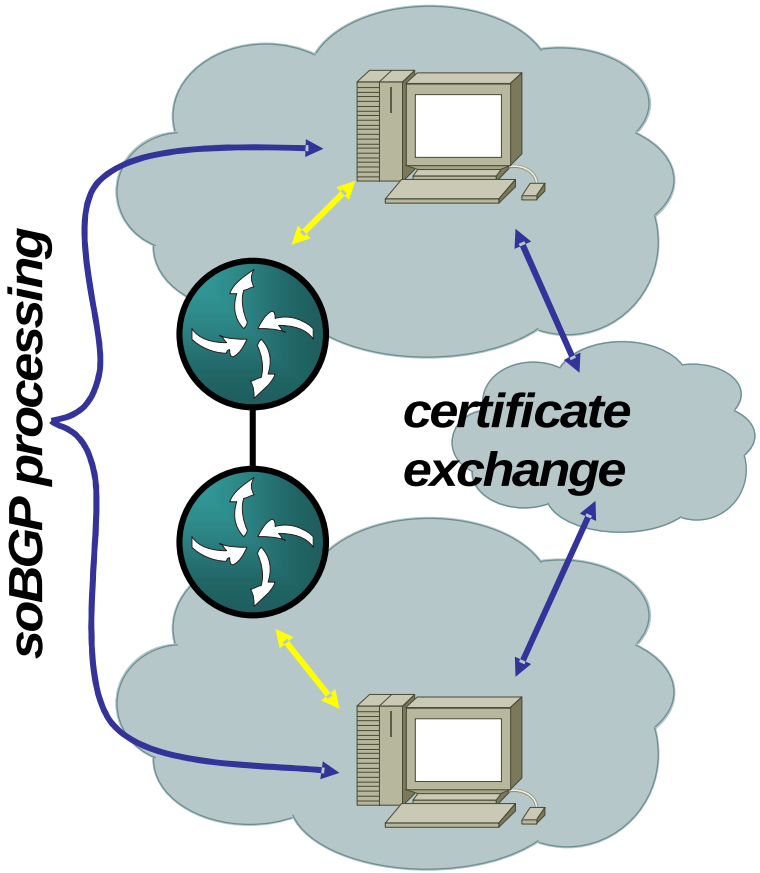
Deployment Options

- サーヴァー同士が、multihop eBGPでcertificateの交換することも可能。



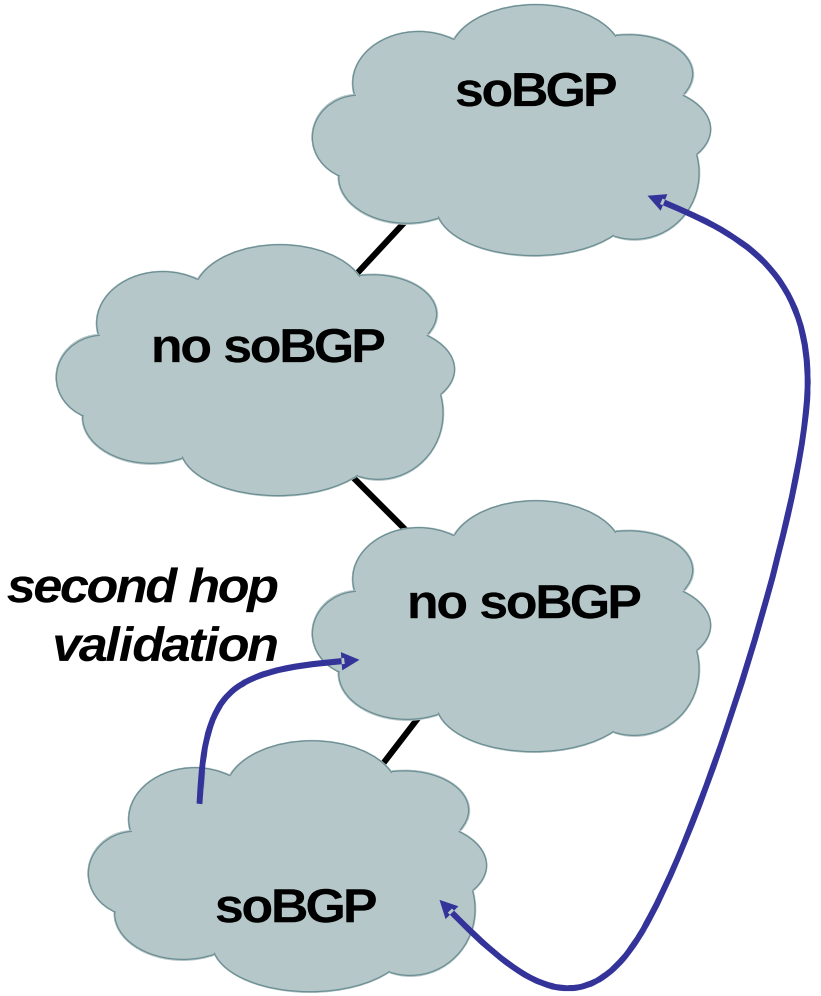
Deployment Options

- ある種のthird party機関を介してcertificateの交換をすることも可能。
- Validation processが同一であれば、certificateの交換方法はどのような手法であっても良い。



Incremental Deployment

- **SO-BGPを運用したい2つのASは、eBGP multihopや、他の方法を使って、certificateの交換をする。**
- **各ASは、それぞれのcertificateに基づきvalidationし、またそれぞれのcertificateに基づきupdateする。**
- また、PolicyCertsにより広報されたconnectivity情報により、AS Path中のsecond hopのvalidateを行なうことも可能。
- より多くのASが参加すれば、より多くのPATHがvalidationされる。

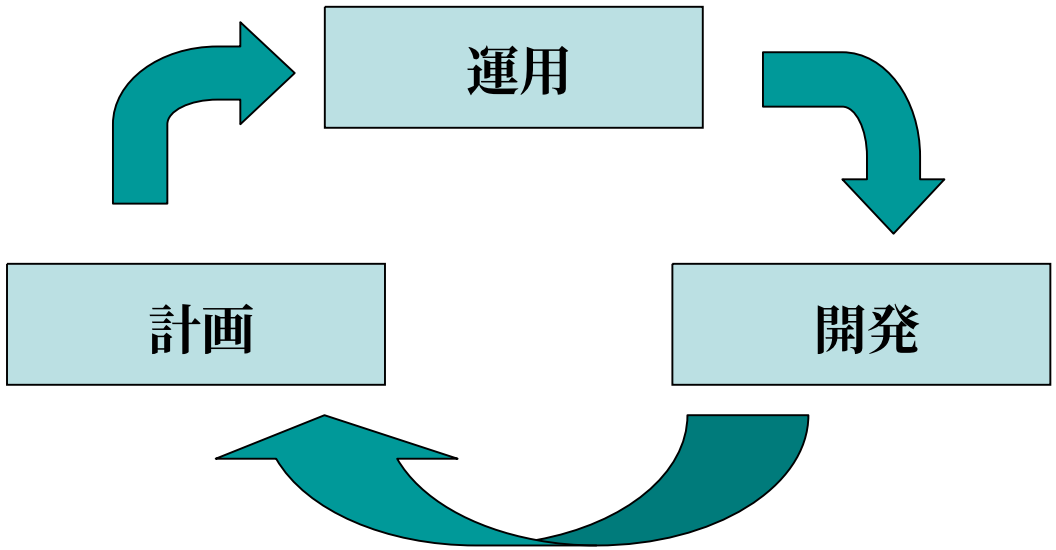


SO-BGP

- 本当に必要かどうか、実装・運用に値するかどうかはわからない。

最後に

- **Inter-domain securityは、各組織が利害を超えて取り組んで行く必要がある最たる分野。**
- **良きfeedback loopを作りたいと思います。**



Thank you!