(D)DoS 対策いろいろ

シスコシステムズ株式会社
アライアンス＆テクノロジ
横山晴庸 (hyokoyam@cisco.com)

アジェンダ

- DDoS？
- Cisco DDoS対策製品(旧Riverhead社製品)
  - 動作概要
  - 内部の防御の仕組み
  - 導入時構成
- 使ってますか？利用可能(かもしれない)DDoS対策
  - uRPF再び(三たび？)
  - Remote Triggered Black Hole
  - IP source tracker
  - Netflow/sFlow等の管理データの攻撃検知への利用

DDoS?

- クライアント/サーバー型
  - コントローラ/ゾンビ(エージェント)型。
  - Worm,不正コピーソフトに忍ばせたトロイ等でゾンビを作成。
  - IRCをリモコンがわりに使った操作。BOTnet。
- 人海戦術でツール利用。
  - 仲間を募ってツールを配り一斉にドン。
  - 田代砲とか…
- Reloadの繰り返し
  - F5アタック。速報サイト等は悪意なくやってしまうケースもあるかも。

特性

- 準備には(ゾンビを増やす際)脆弱性を利用するが、DDoS攻撃そのものは脆弱性を突いてくる訳ではない
  - –DDoSの攻撃対象にされるような立派なサイトはパッチもしっかり管理されているケースが多いハズ。
- トラフィック量は異常でも、Flowの性格自体は普通のアクセスと似ている場合が多い。
  - –個々のFlowだけを見て識別するのは容易ではない。

Refference

- **Distributed Denial of Service (DDoS) Attacks/Tools**
  http://staff.washington.edu/dittrich/misc/ddos/
- **DDoS World** **http://www.ddosworld.com/**
- **[Bots & Botnet: An Overview] SANS Institute 2003**
  http://www.sans.org/rr/whitepapers/malicious/1299.php

DDoS対策製品(旧Riverhead社製品)

- Cisco DDoS対策製品(旧Riverhead社製品)
  - 概要
  - 内部の動作の仕組み
  - 導入時構成、使われ方

Cisco DDoS 対策製品

- DDoS攻撃を受けたとしてもサービスを継続させるという点に主眼をおいている。
  - –攻撃されてる間でも一般ユーザーに対しては継続してサービスするという事が目標。
  - –不正なトラフィックを全て遮断する訳ではない。
- “正常でない”トラフィックを検知。
- ネットワークでのサービス(Webアプリケーション、DNSその他)をDDoSから守るのが主目的。
- 攻撃の検知をするアプライアンス、攻撃の分析と緩和をするアプライアンスの2種類により構成。
  - –検知 Cisco Traffic Anormaly Detector XT5600
  - –緩和処置 Cisco Guard XT5650

製品

2種類のアプライアンス。

Anomaly Detectorで検知し、Guardで攻撃を止める

Cisco Guard XT 5650:

攻撃の分析と緩和

攻撃発生時にトラフィックを自分自身を通過するよう迂回させる

Cisco Guard XT 5650

Cisco Traffic Anomaly Detector XT 5600:

トラフィックの分析を行いAlertを送る。

Tap, SPAN等でトラフィックを受信

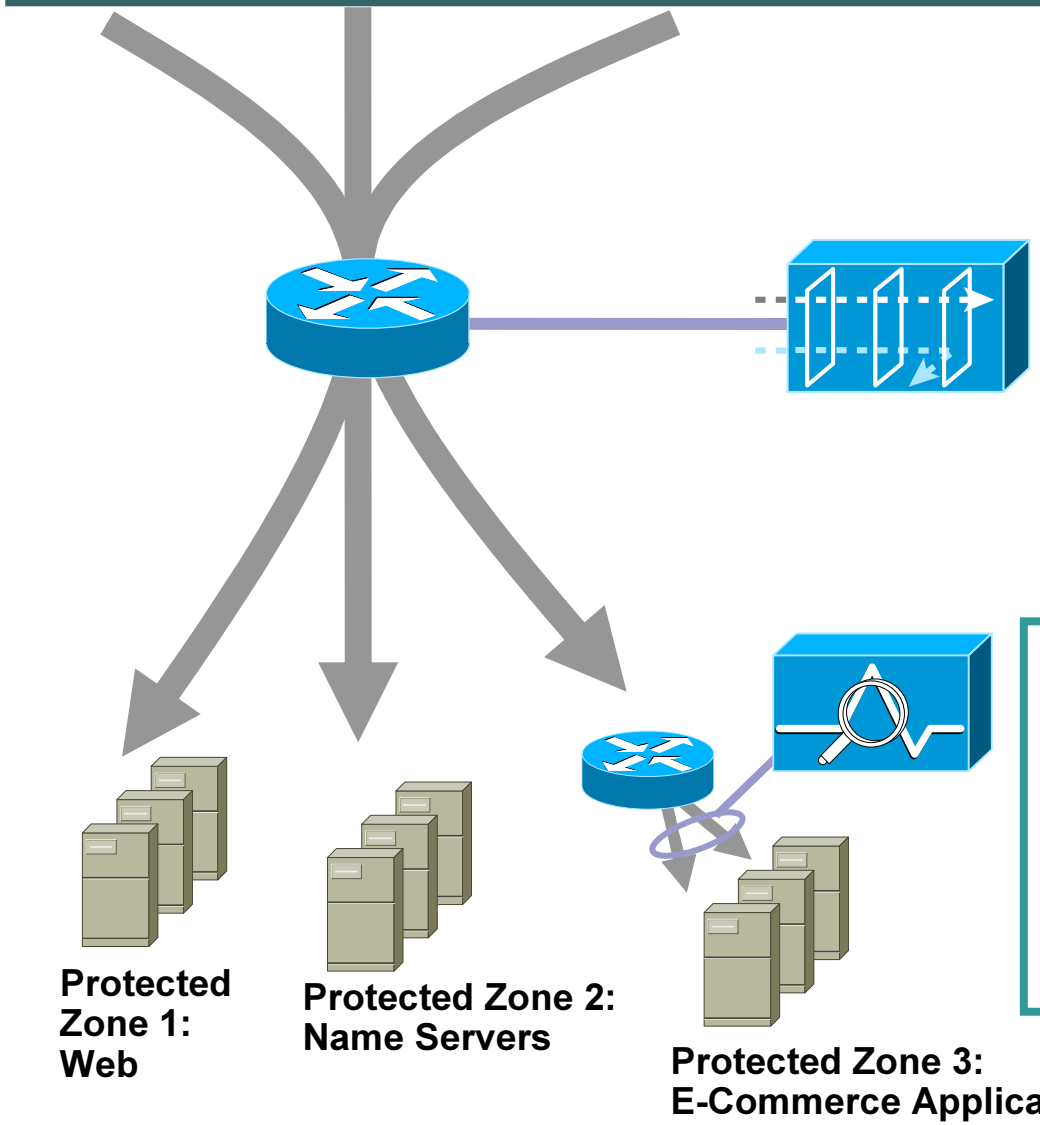
Cisco Traffic Anomaly Detector XT 5600

2RU

管理用IF 1000B-T

データ用IF 1000B-T/SX/LXの選択

各コンポーネントの役割



Cisco Guard XT

Anomaly Detectorからイベントをうけて動作する。

通信に介入する事でより詳細な検査を実施。攻撃トラフィックは落とす。

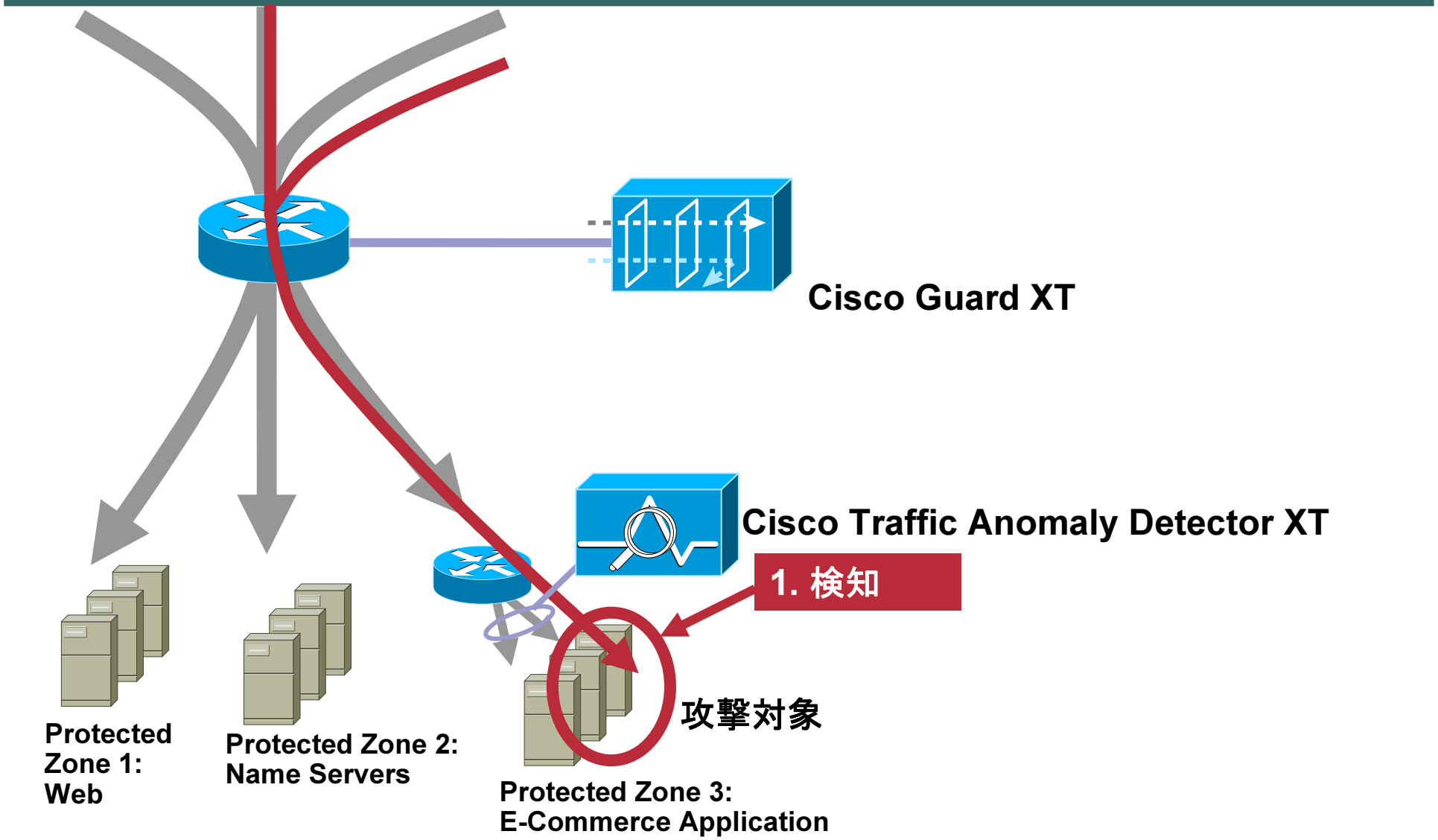
Cisco Traffic Anomaly Detector XT

TAP,SPAN等で常時トラフィックを監視。

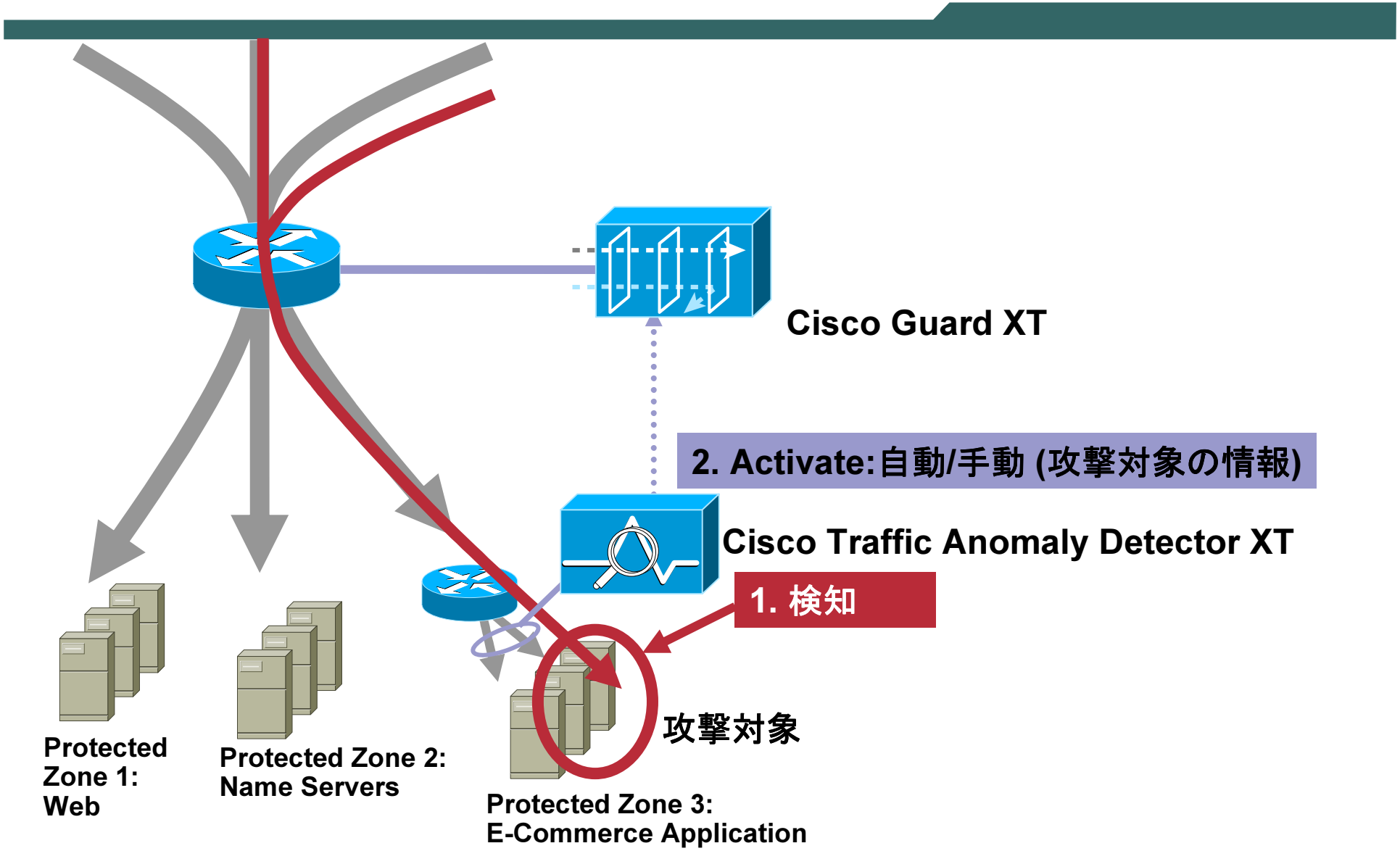
攻撃の兆候があったらGuardにどのサービスが攻撃を受けてるかをDst IP ベースで知らせる。

通信には影響しない。

Diversion Architecture



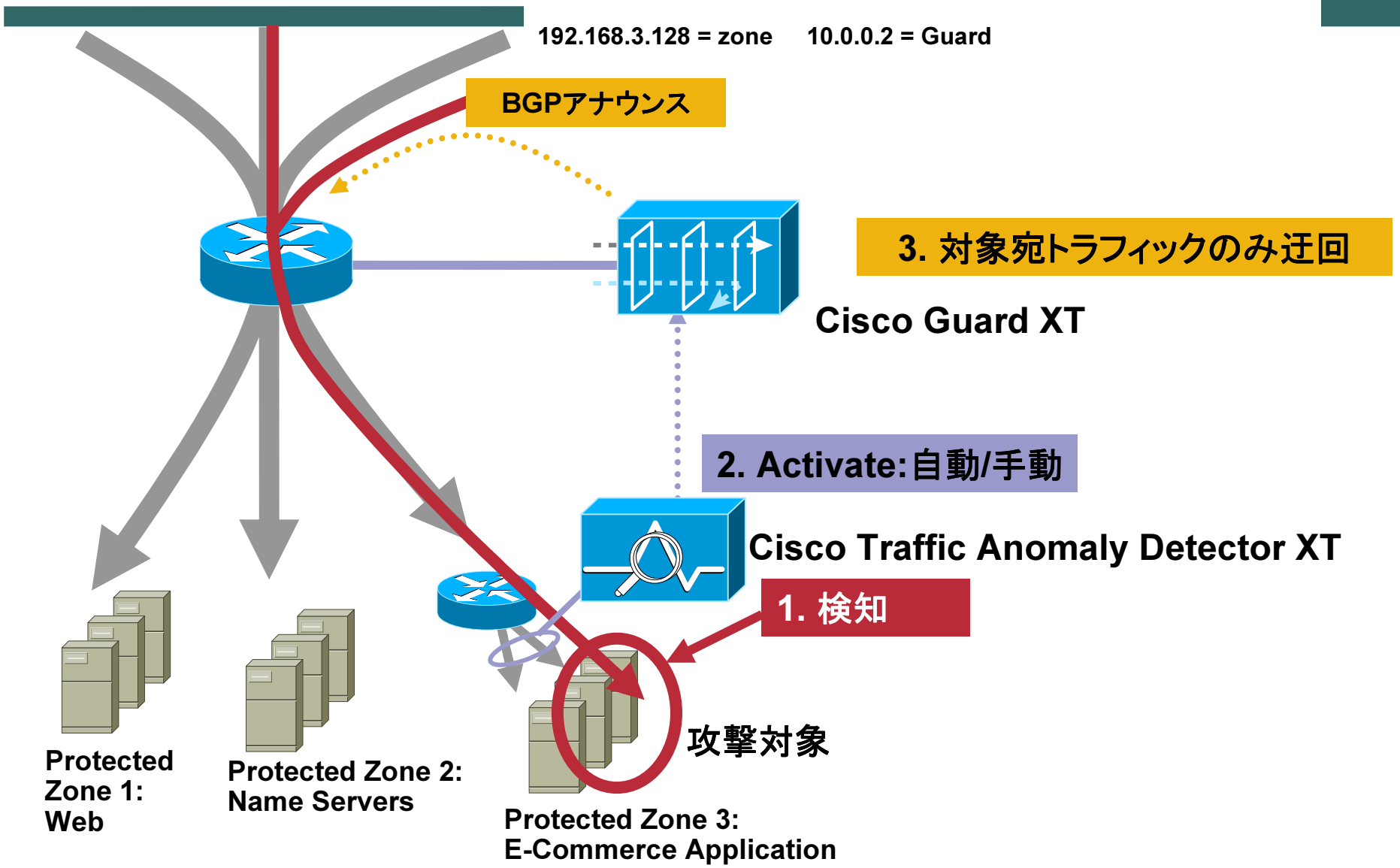
Diversion Architecture



Diversion Arcl

O 192.168.3.0/24 [110/2] via 10.0.0.3, 2d11h, GigabitEthernet2
B 192.168.3.128/32 [20/0] via 10.0.0.2, 00:00:01

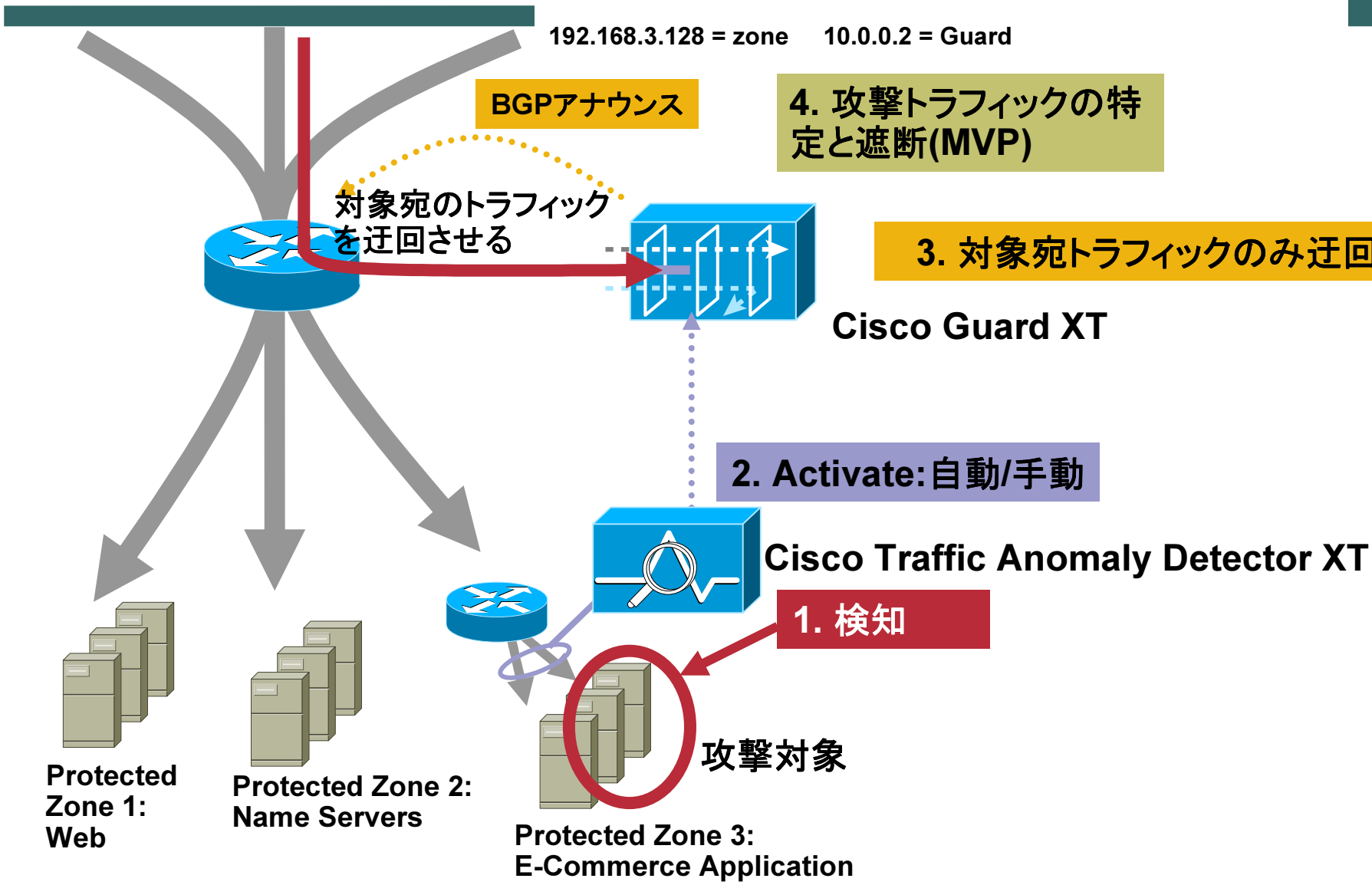
192.168.3.128 = zone 10.0.0.2 = Guard



Diversion Arcl

O 192.168.3.0/24 [110/2] via 10.0.0.3, 2d11h, GigabitEthernet2
B 192.168.3.128/32 [20/0] via 10.0.0.2, 00:00:01

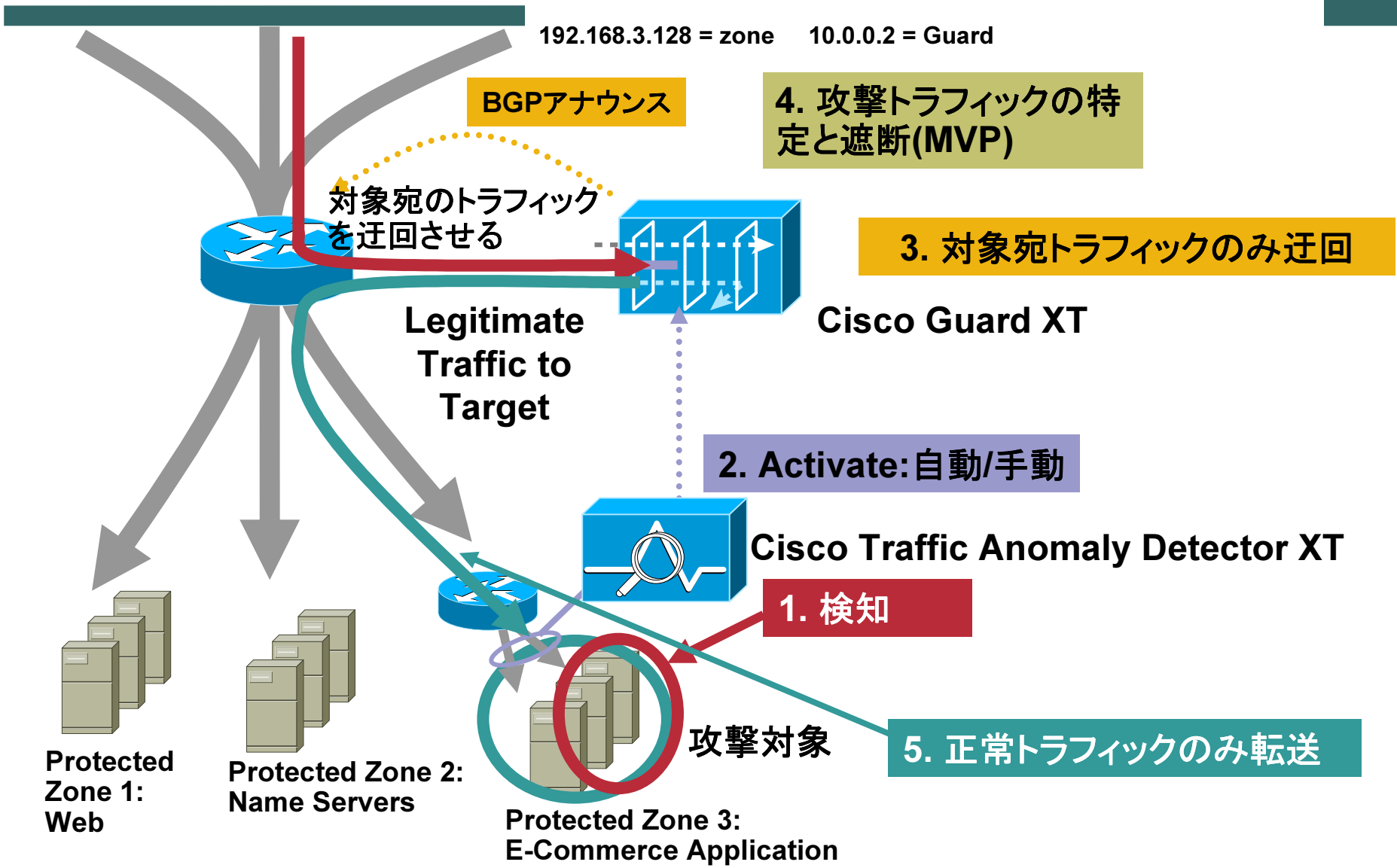
192.168.3.128 = zone 10.0.0.2 = Guard



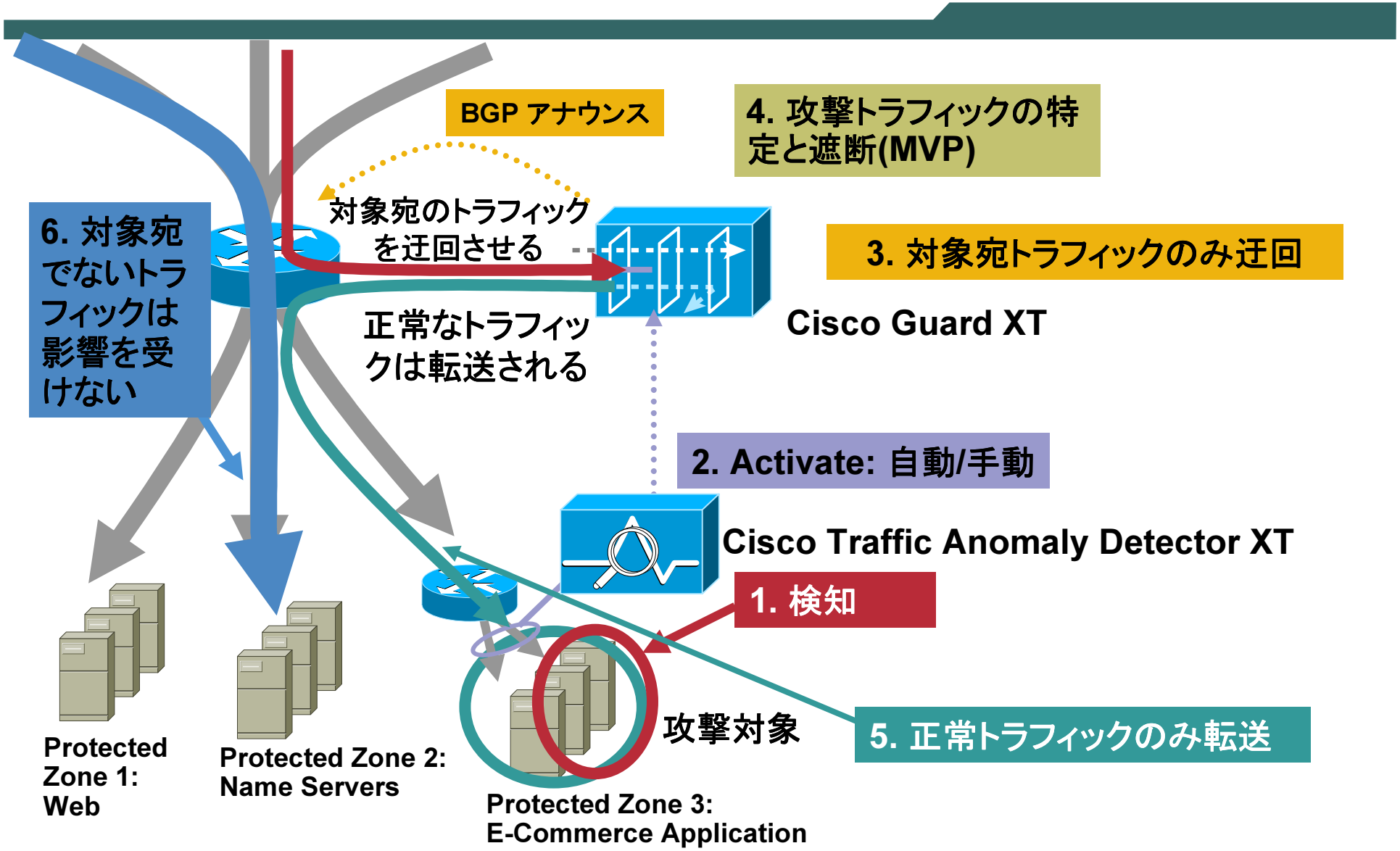
Diversion Arcl

O 192.168.3.0/24 [110/2] via 10.0.0.3, 2d11h, GigabitEthernet2
B 192.168.3.128/32 [20/0] via 10.0.0.2, 00:00:01

192.168.3.128 = zone 10.0.0.2 = Guard

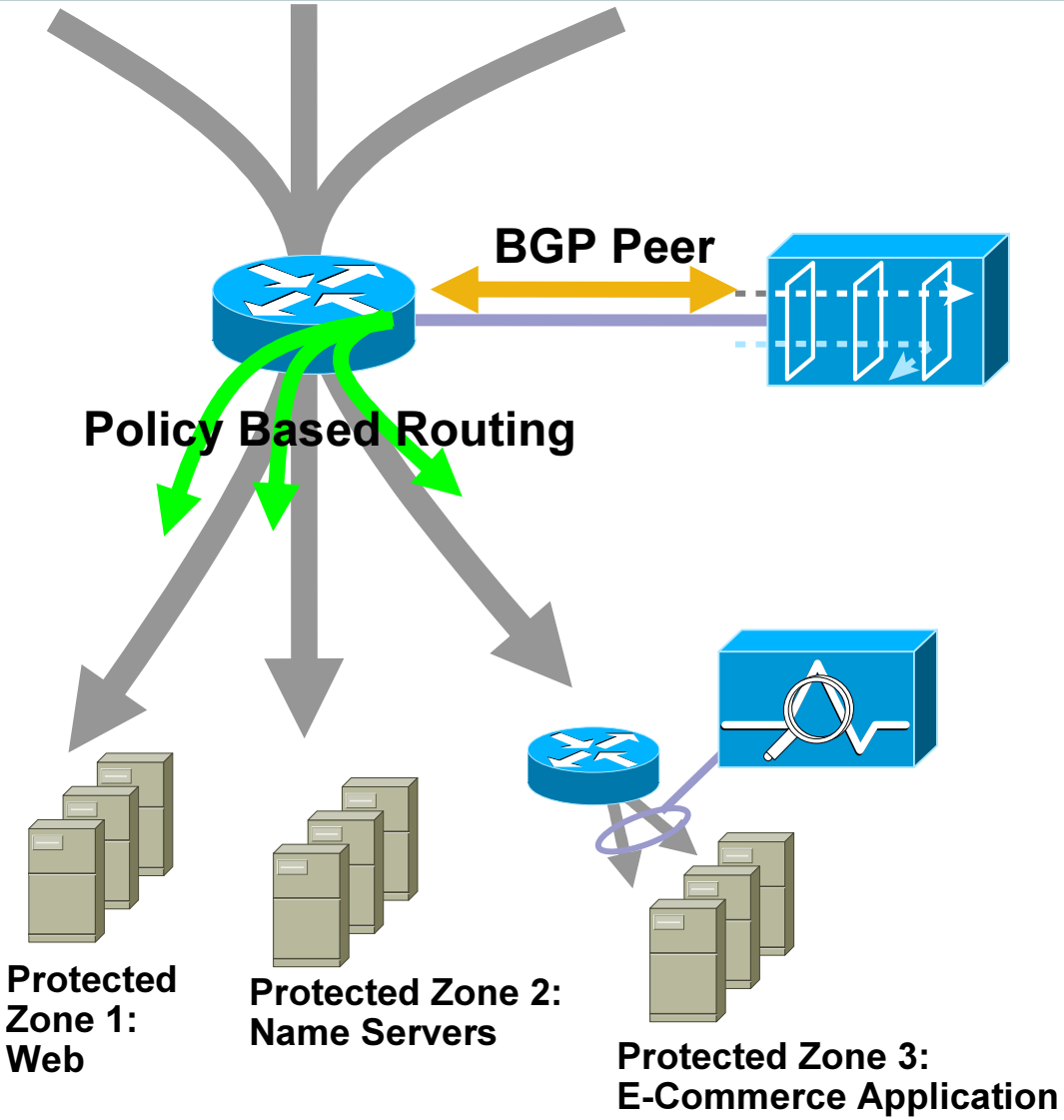


Diversion Architecture



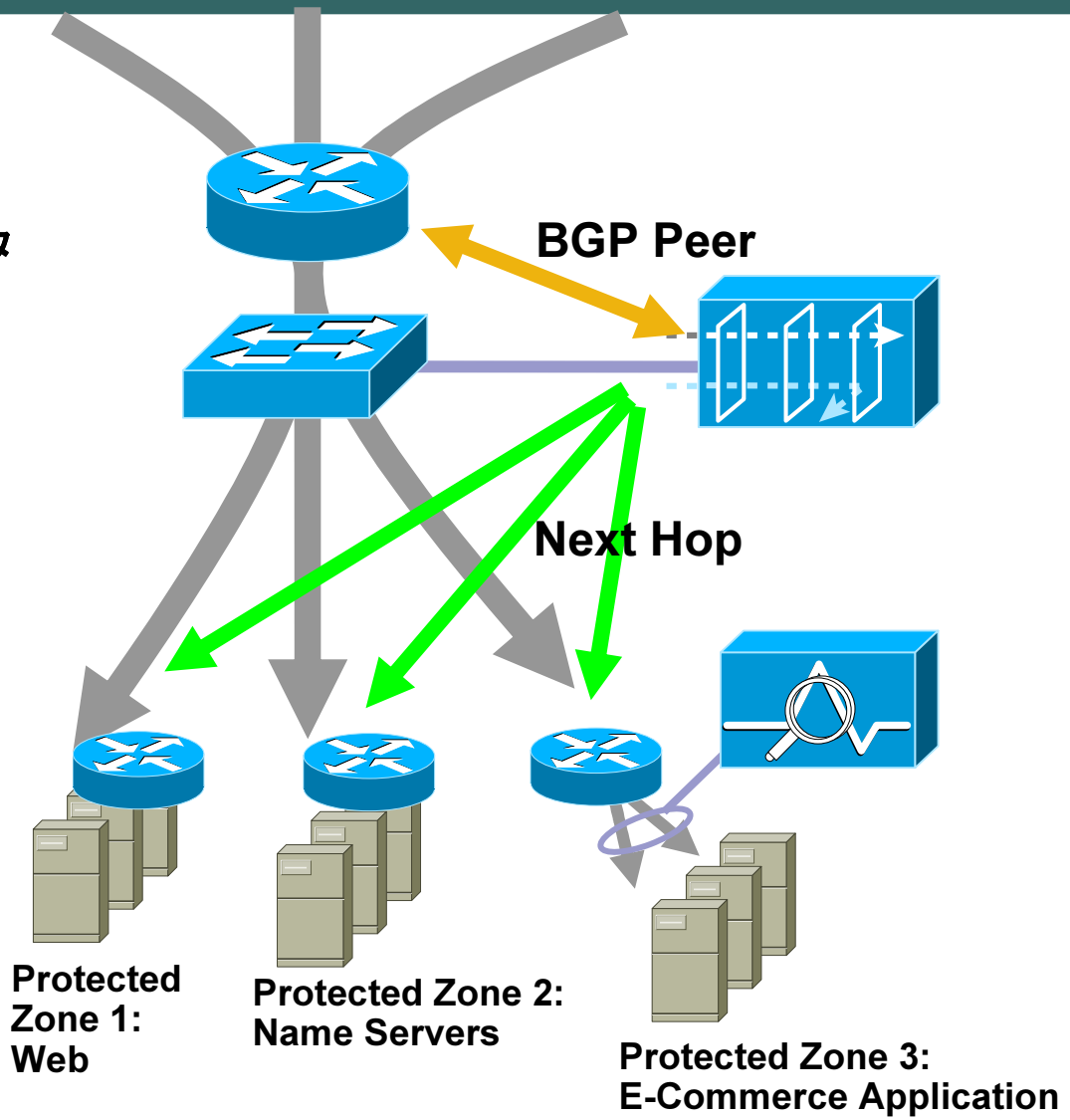
L3構成例

- Uplinkのルーターに横付け
- Policy Routingで転送



L2構成例

- Uplinkのルーター下のL2セグメントに設置
- Guardから見て下位のルーターがNext Hopになる。

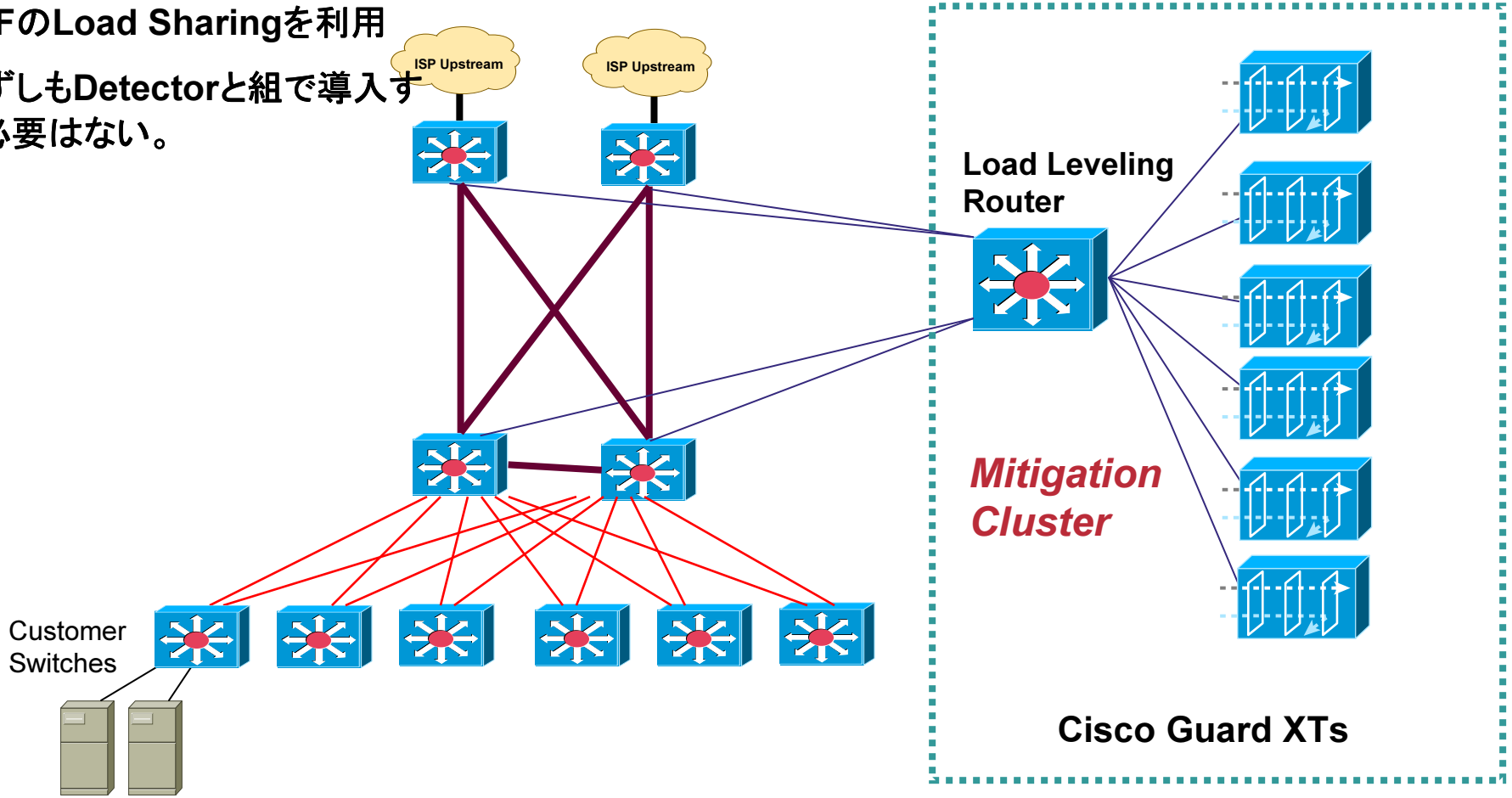


広帯域対応クラスタ構成

1Gbpsを超えるようなリンクで
はクラスタリングで対処。

CEFのLoad Sharingを利用

必ずしもDetectorと組で導入す
る必要はない。



処理の流れ概要

- 運用に先立ってTrafficのLearningを実施
  - –Anomalyを識別するために、正常時の状態を学習する。
  - –Policy Construction (流れているトラフィックを確認する)とThreshold Tuning (適正な値に閾値を設定する)の2段階。
  - –保護対象Zone毎にTrafficのプロファイルを作成する。そのプロファイルから逸脱するトラフィックがAnomaly。
- Anomaly通信は統計項目単位で検査、遮断を実施
- Multi-stage Verification Process手法を使って攻撃トラフィックを落とす。

Multistage Verification Process™ (MVP)

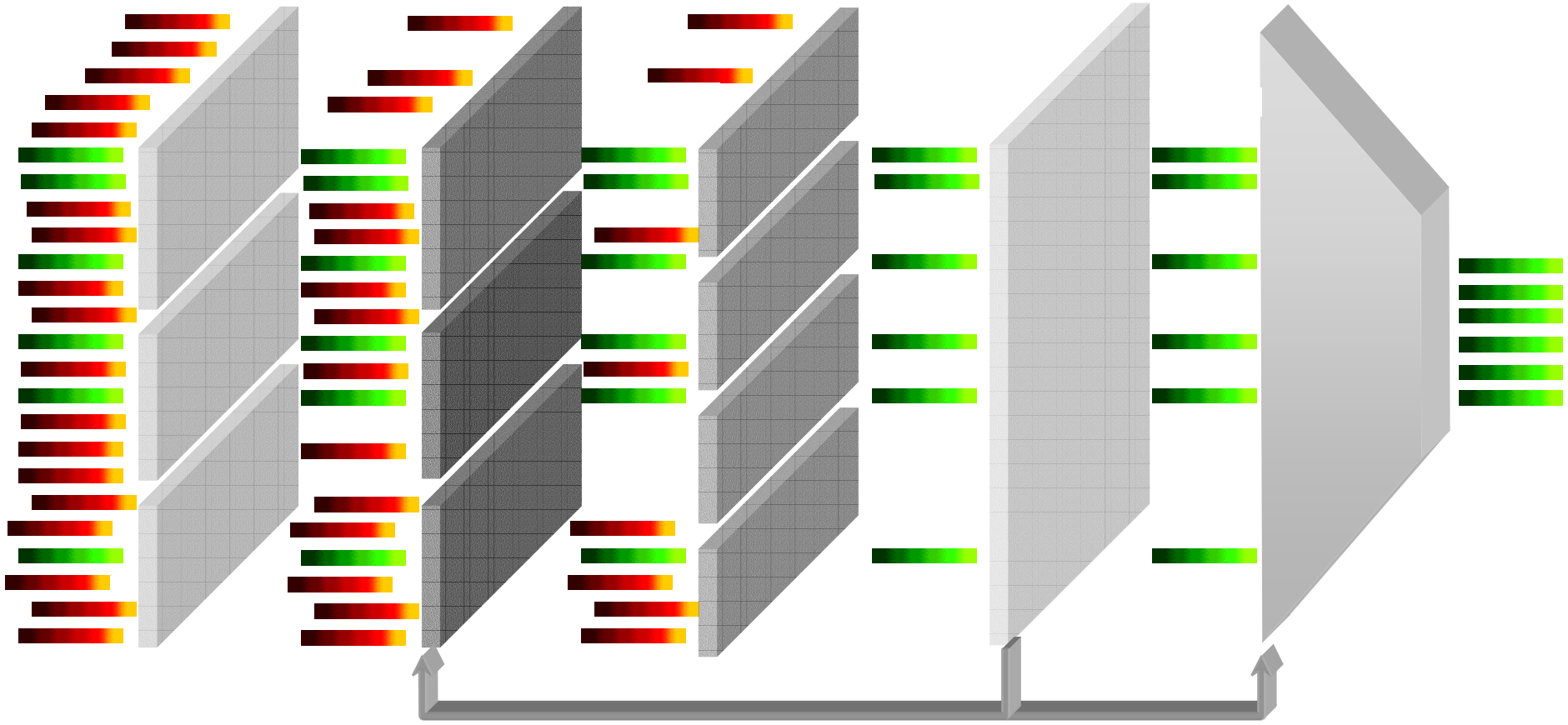
スタティックフィルタ
filter out packets according to pre-defined rules

ダイナミックフィルタ
filter out packets Per Flow, Protocol, Source IP

Anti-Spoofing手法
filter out packets from spoofed sources

統計情報による検査
Anomaly Recognition per flow compared to a baseline

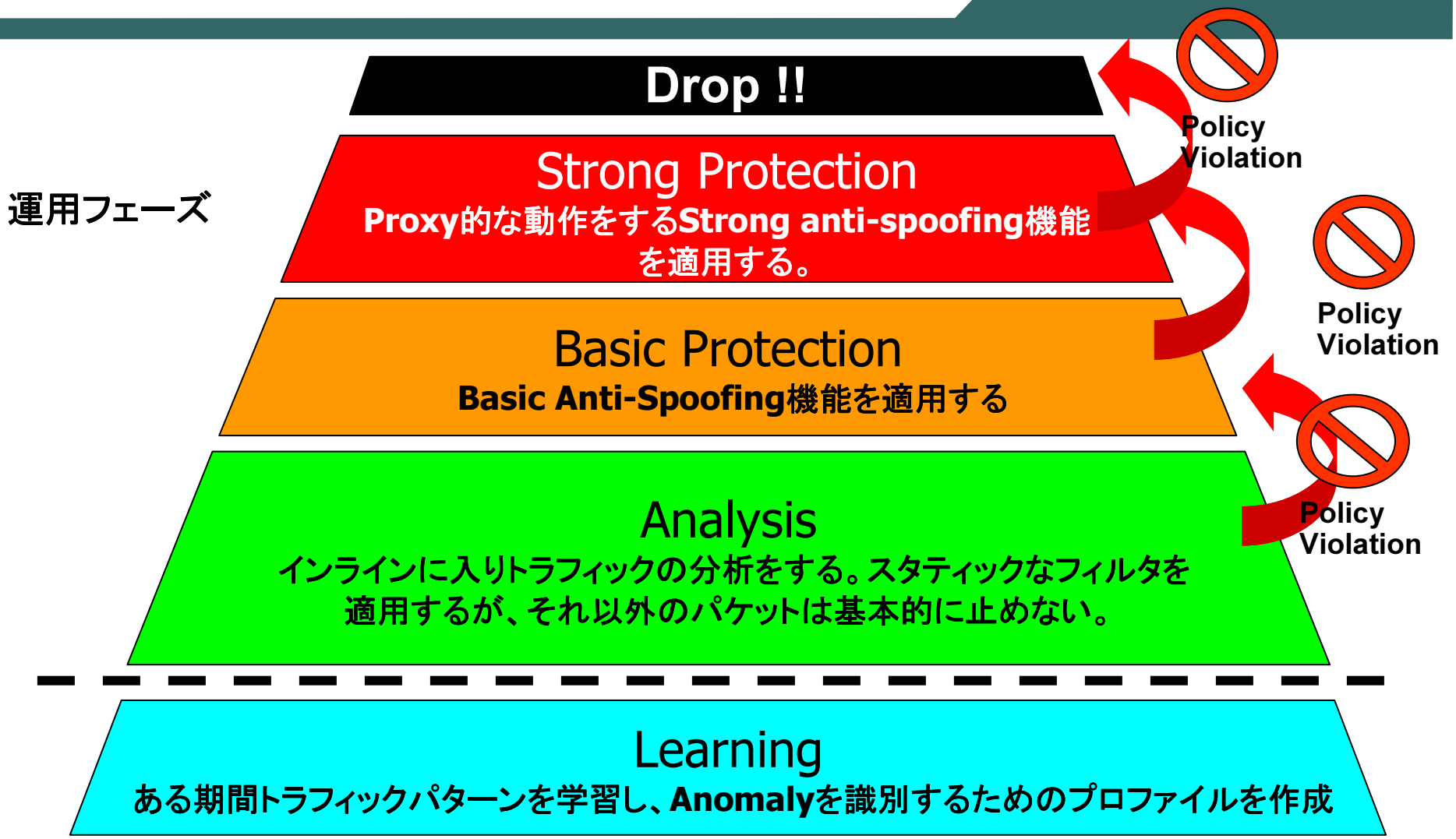
Rate Limitting
of traffic towards the zone



Anti-Spoofing手法

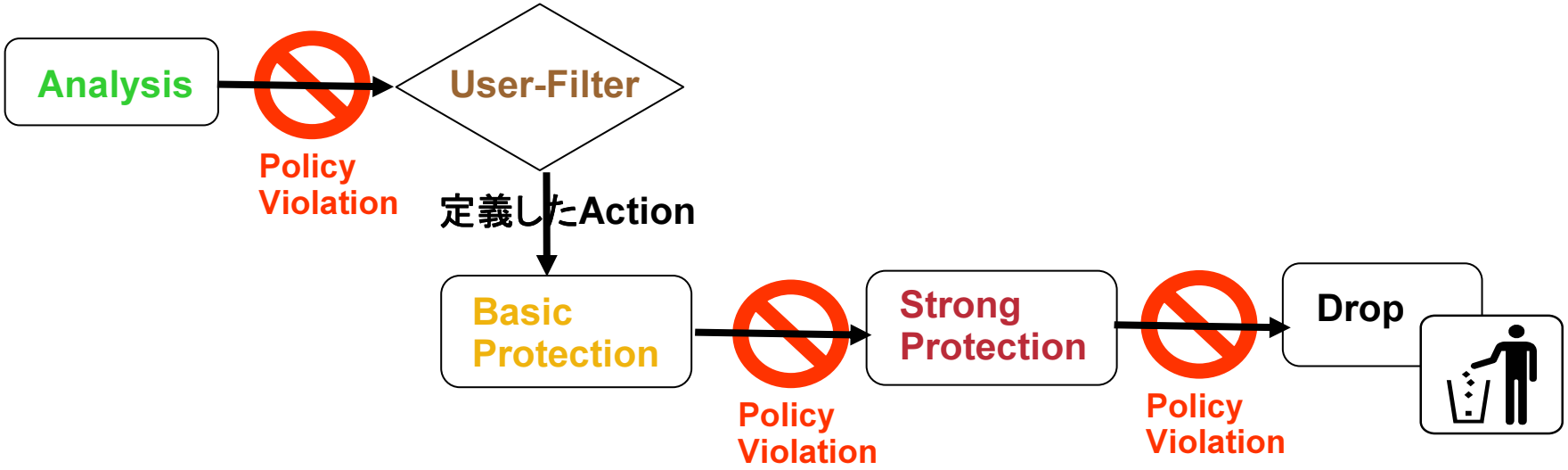
- プロトコル毎に別の手法を利用している
  - HTTP, DNS, SMTP, IRCなど
- 接続元の有効性を確認する
  - 正規TCPパケット（SYN、SYN/ACKs、FINs）
  - DNS リクエスト、DNS リプライ、Zone transfers
  - コントロールセッションに関連されたUDPトラフィック
- プロトコルとレベル(Analysis,Basic,Strong)によって違う手法を適用する
  - SYN cookie
  - Safe reset
  - TTL
  - DNS Authentication
  - リダイレクト

Anti-Spoofingのレベル



HTTPトラフィックの例

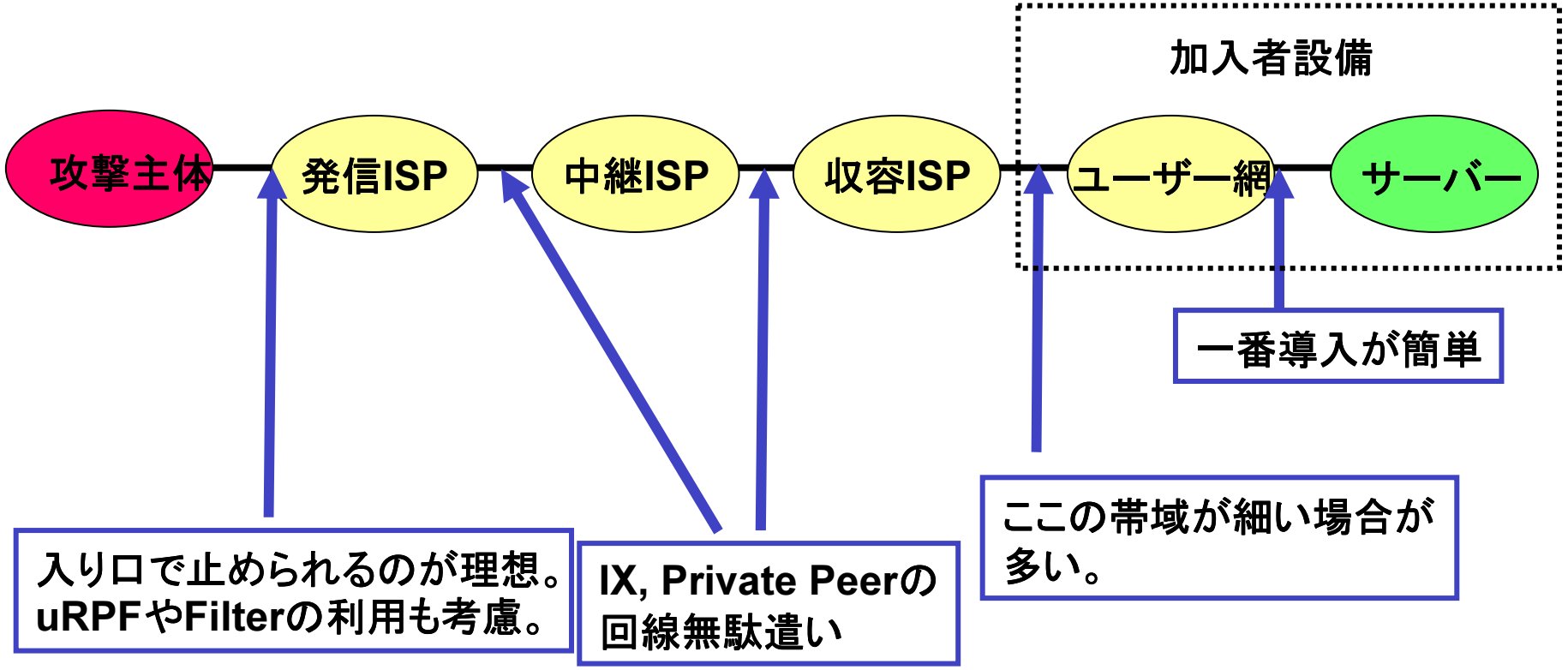
Policy	State	IStatus	Threshold	Proxy	List	Action	Timeout
http/80/analysis/syns/src_ip	act	a-accpt	4.0	-	0	to-user-filters	600
http/80/basic/syns/src_ip	act	a-accpt	2.0	-	0	filter/strong	600
http/80/strong/syns/src_ip	act	a-accpt	5.0	-	0	filter/drop	600



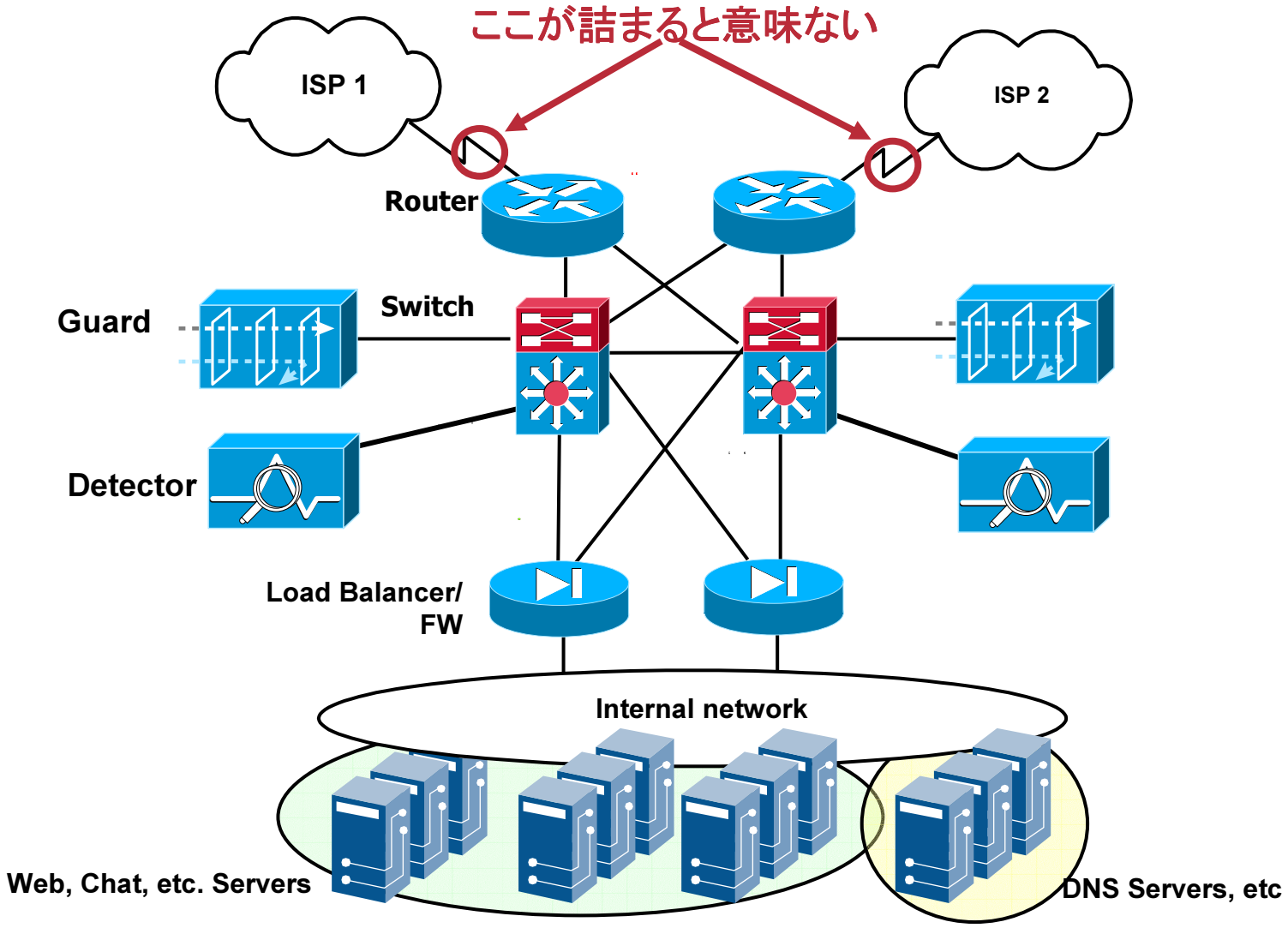
Real Life Examples

攻撃の道のり

- コストが高い線に無駄なトラフィックを流したくはない。
- なるべく入り口に近いところで止めたい。



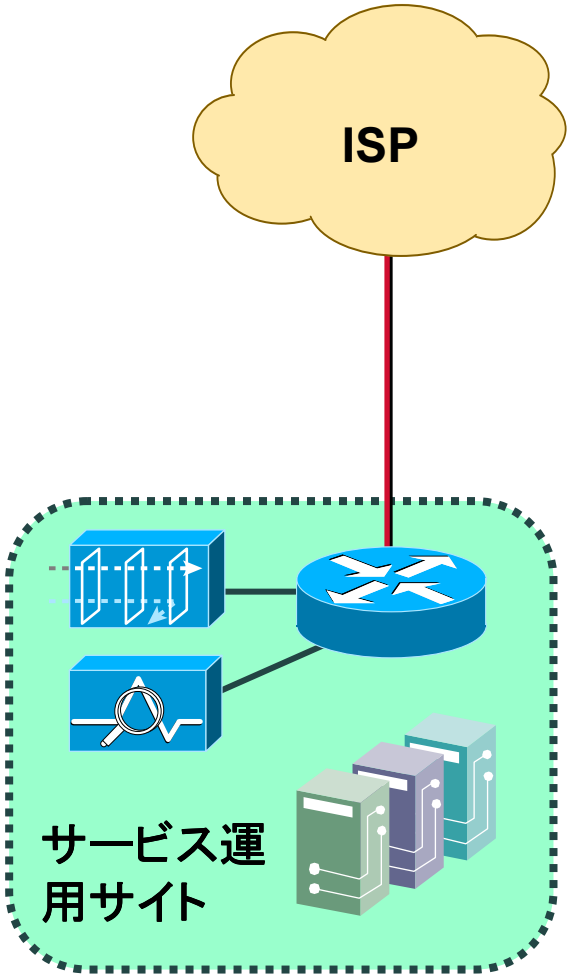
構成例


ここが詰まると意味ない
ISP 1
ISP 2
Router
Guard
Switch
Detector
Load Balancer/
FW
Internal network
Web, Chat, etc. Servers
DNS Servers, etc

構成における悩み

- 責任分界点
  - –管理は誰が行うのか？ISPが設備を持つのか、加入者なのか？
  - –誰が検知するのか、誰がトラフィックの迂回を決断するのか、誰が攻撃トラフィックを落とすのか？
- 攻撃対象にされる部分は何なのか？
  - –DNS,Web,SMTP等の各種のサービス(End Point)なのか?
  - –細いリンク帯域の輻輳なのか？
- トラフィックの迂回法
  - –上位のルーターとの間でBGPが張れるのか？
  - –自動かInteractiveか？
  - –誰が迂回の決断をするのか？

ISPの助けを借りないモデル



メリット

•ISP側と交渉する必要がない。

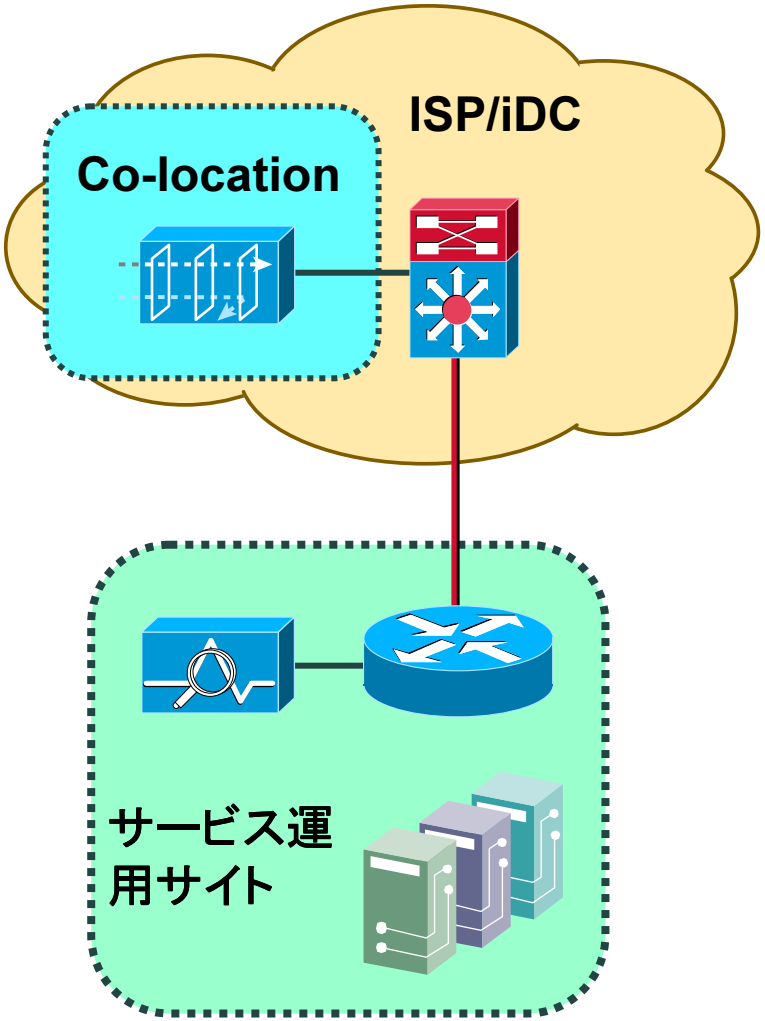
•運用を完全に制御できる。

デメリット

•リンクの帯域が消費されるような攻撃に対しては有効ではない。

•攻撃をうける頻度が多ければ運用の負荷は大きい。

GuardをISP/iDC内にco-locationするモデル



メリット

•攻撃トラフィックをISP網内で止められるため、アクセス線が無駄遣いされる事がない。

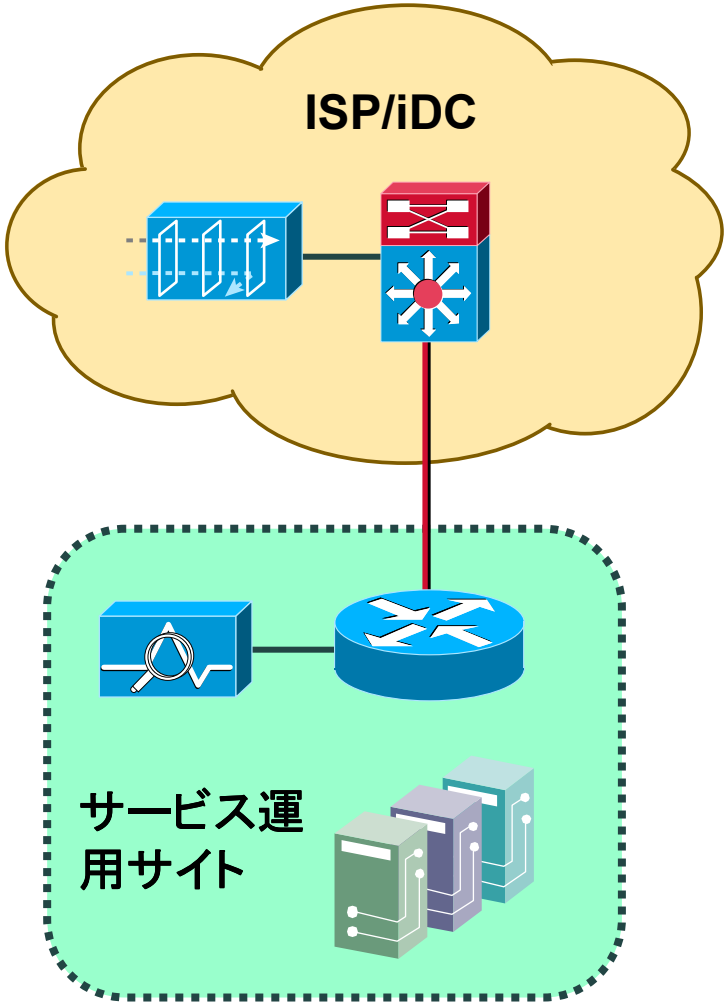
•Guardまで自分の管理下なので細かく制御可能。

デメリット

•ISPのエッジルーターに対してBGPでPeeringする必要があり、特別に対応してもらう必要がでてくる。

•Co-Locationスペースに費用がかかる。

GuardをISP/iDCがサービスするモデル



メリット

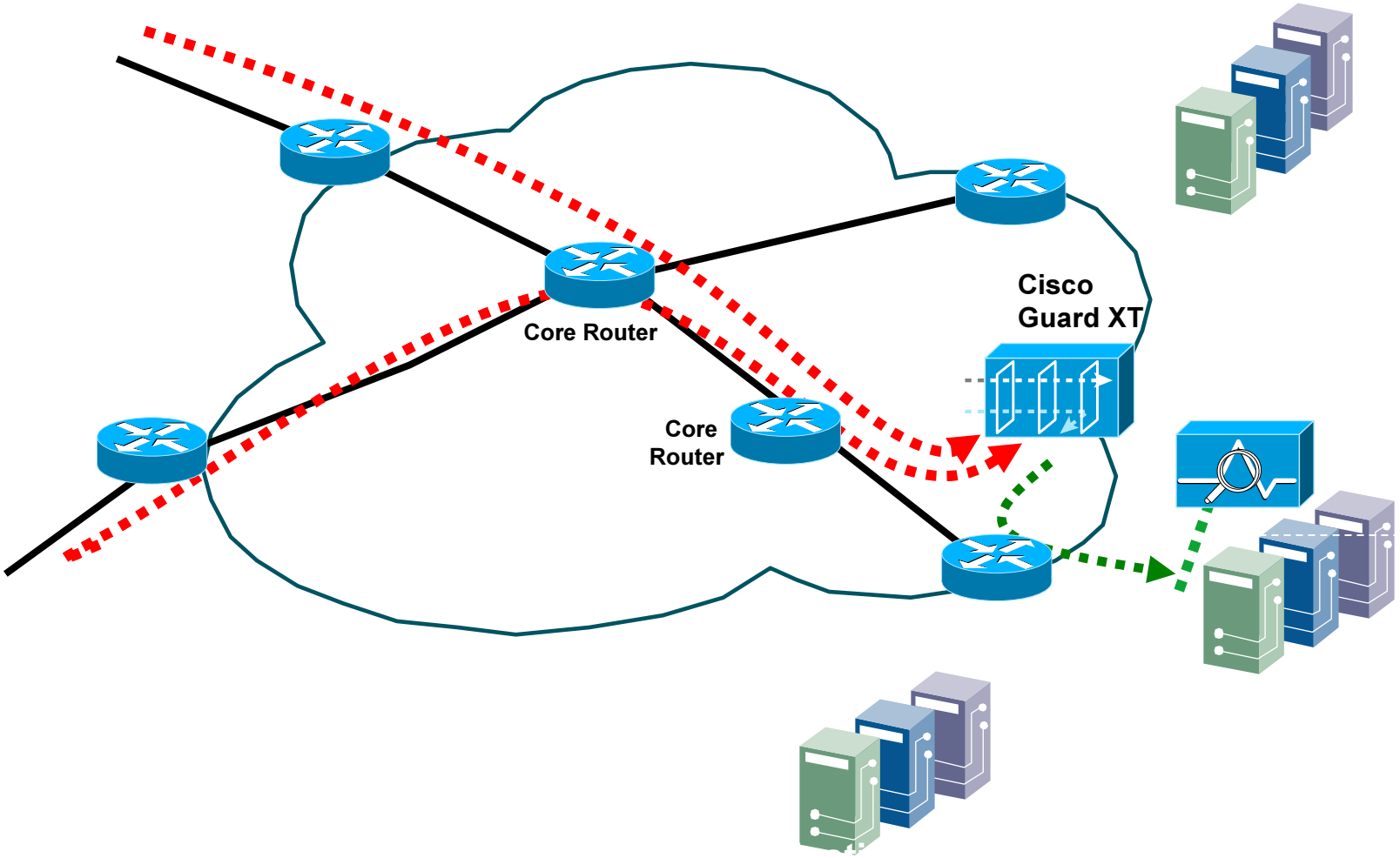
•攻撃トラフィックをISP網内で止められるため、アクセス線が無駄遣いされる事がない。

•運用の工数は減らせる。

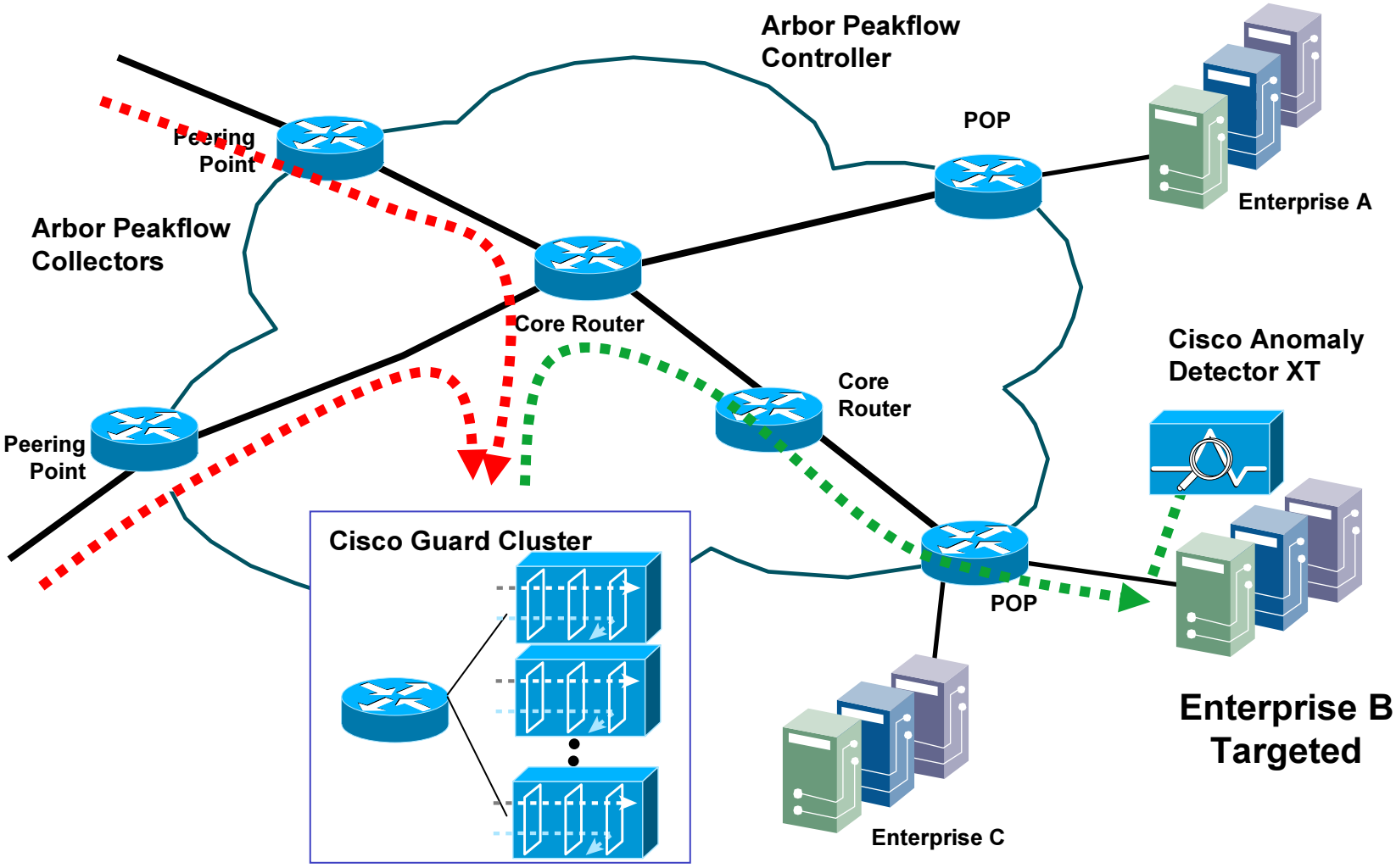
デメリット

•Guardの運用に関してはISPに依存する形になるのでユーザーが細かく制御するのは難しい。

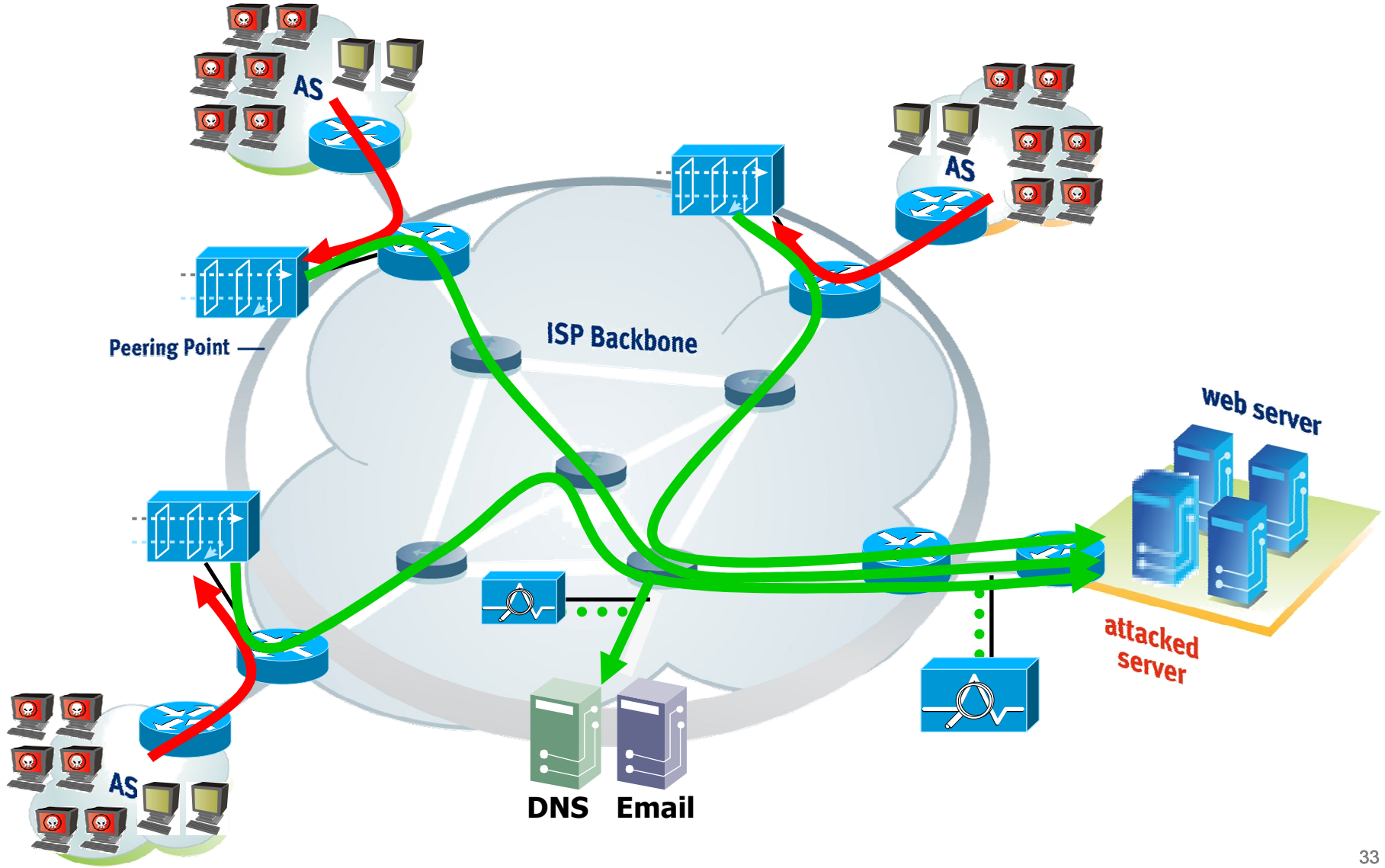
ISPによるProtectionサービス
Distributed/Edge Protection



集中処理型


Arbor Peakflow
Controller
POP
Enterprise A
Peering
Point
Arbor Peakflow
Collectors
Core Router
Cisco Anomaly
Detector XT
Core
Router
Peering
Point
Cisco Guard Cluster
POP
Enterprise B
Targeted
Enterprise C

Peering Points置き



製品概要まとめ

- DDoS攻撃の検知、緩和の実施
  - 攻撃検知、緩和の自動実行
  - インフラの安定性を実現
  - 正規アクセスユーザーに対するサービスの継続
- 非インラインデバイス
  - 導入リスクが少ない
  - 必要な時だけインラインに…
  - クラスタリング構成も可能

Refference

- **[Cisco Traffic Anomaly Detectors]**
  http://www.cisco.com/japanese/warp/public/3/jp/product/hs/security/tad/
- **[Cisco Guard DDOS Mitigation Appliances]**
  http://www.cisco.com/japanese/warp/public/3/jp/product/hs/security/gdma/

その他のISP security対策

- uRPF再び(三たび？)
- Remote Triggered Black Hole
- IP source tracker
- Netflow利用の攻撃検知

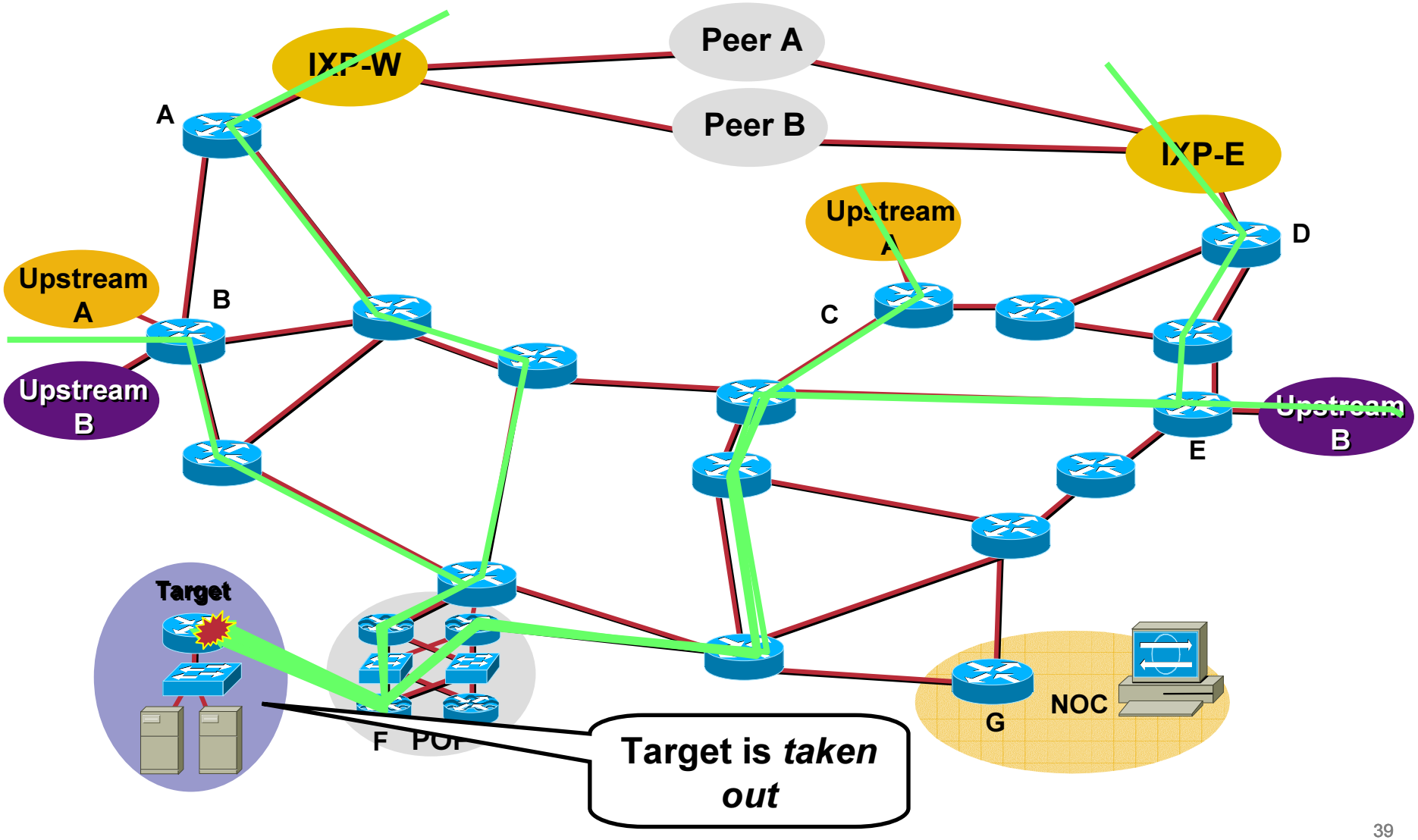
uRPFの適用

- **Strict Mode**
  - –エッジ加入者を収容しているルーターに適用して、Source address Spoofingを防止。
- **Loose Mode**
  - –他ISPと接続しているルーターに適用
  - –完全ではないが、明らかなアドレス詐称の防止にはなる。(Bogon Listをメンテするより良さそうな)
  - –Source BaseのRTBHのため

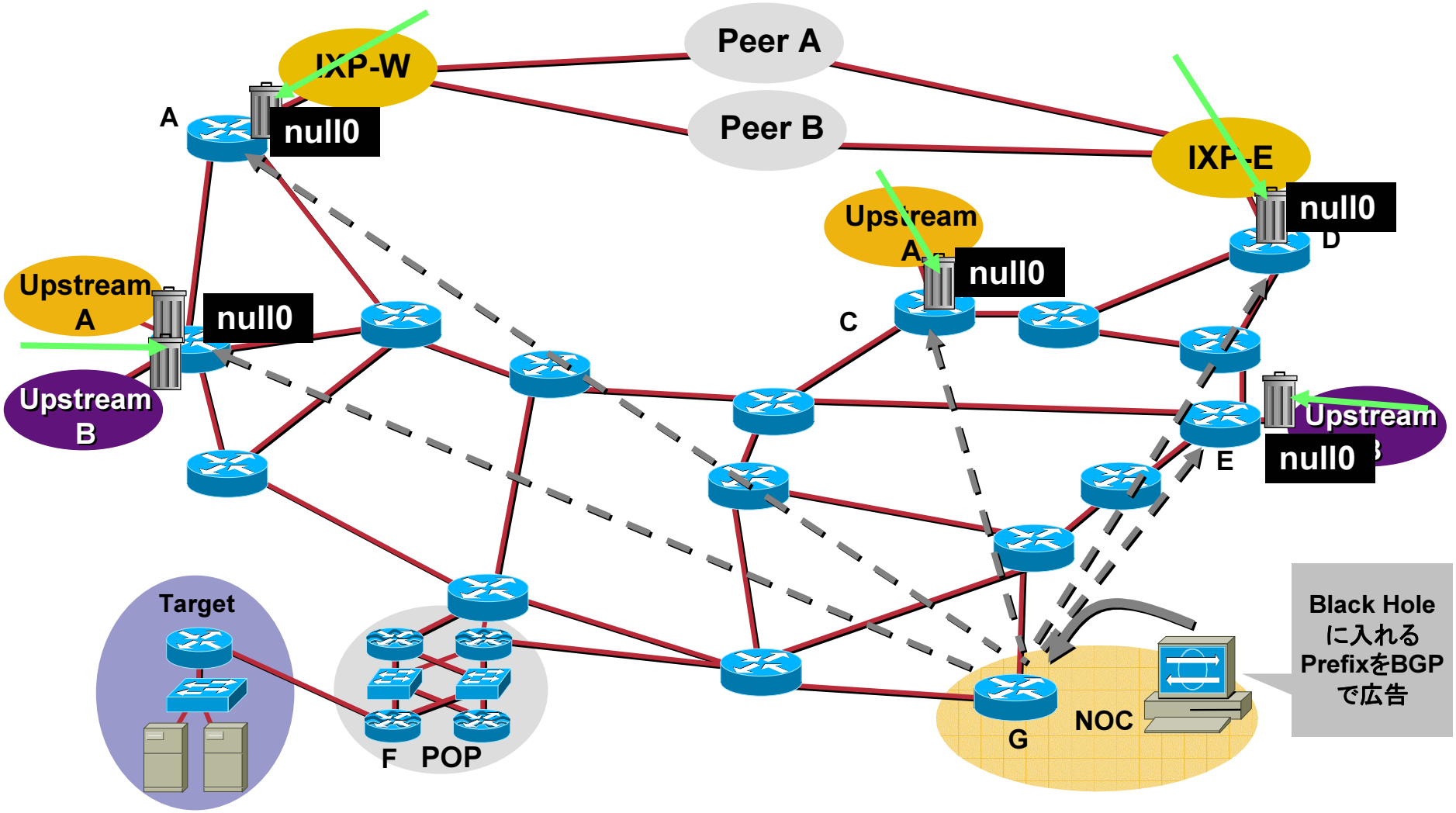
Remote Triggered Black Hole Filtering

- 攻撃トラフィックを網の入口で捨てるために利用
- BGPを利用してエッジのルーターにお知らせ
- 各エッジのルーターに予め設定をしておく必要はあるが、平常時の動作に影響を与えるものではない。
- オペレーション用のルーター(攻撃発生時に防御をトリガするルーター)と各エッジルーターの間でBGPを張っておく。

DDoS攻撃時


IXP-W
Peer A
Peer B
IXP-E
A
B
C
D
E
F
G
Upstream A
Upstream B
Upstream A
Upstream B
Target
POP
NOC
Target is *taken out*

Remote Triggered Black Holeによる対処



Remote Triggered Black Hole

- 普通にアクセスしたいユーザーもアクセスできなくなってしまう可能性アリ。
- ソースアドレスベースで実行する事も可能。
  - 一長一短あります。
- DNSを利用するケース
  - 応答としてLoop back アドレスやごみ箱行きのアドレスを返して対応。やっぱり皆アクセスできなくなりますね？
- 電気通信事業法の第3条(検閲の禁止)や第4条(秘密の保護)なんかとの絡みは？

RTBH応用 Sourceベース

- uRPF loose modeを利用
- 指定するSource IPアドレスに対するNext-hopに存在しないアドレスを指定する事でuRPFにFailさせる。
- Sourceを個別で指定するのは現実的？

RTBH応用 Communityによるグルーピング

- 基本のRTBH構成にcommunityのチェックを付加
- Triggerをかける時にstatic routeにtagを付けて、tagに応じて違うcommunityを付けてupdateする。
- 属性毎にエッジルーターをグルーピングしておく
  - –海外線のグループ、全エッジルータを含むグループ、過去に攻撃を受けた時にIngressになってたエッジのグループとかregion別とか

↓

- Black Holeが有効になるエッジを制限。

RTBH応用 Customer Trigger BlackHole

- 顧客(Peer先)からBlack HoleTriggerを許可。
- リスクさえ低ければ、オペレーションは楽になりそうですが…
- サンプルはココ http://www.secsup.org/CustomerBlackHole/

IP Source Tracker

- 送信元を正しく追える機能があれば便利
  - –非対称ルーティングやSource Spoofされてるパケットを追いたい。
  - –逆traceroute的な事は無理ですが。
- 対応IOS版
  - –12.3(7)T以降
  - –12.0(21)S 以降GSR
- 攻撃されてる対象のIPアドレスを指定して情報を生成
  - –Ingress IFを表示してくれるので、前のルーターを辿る。

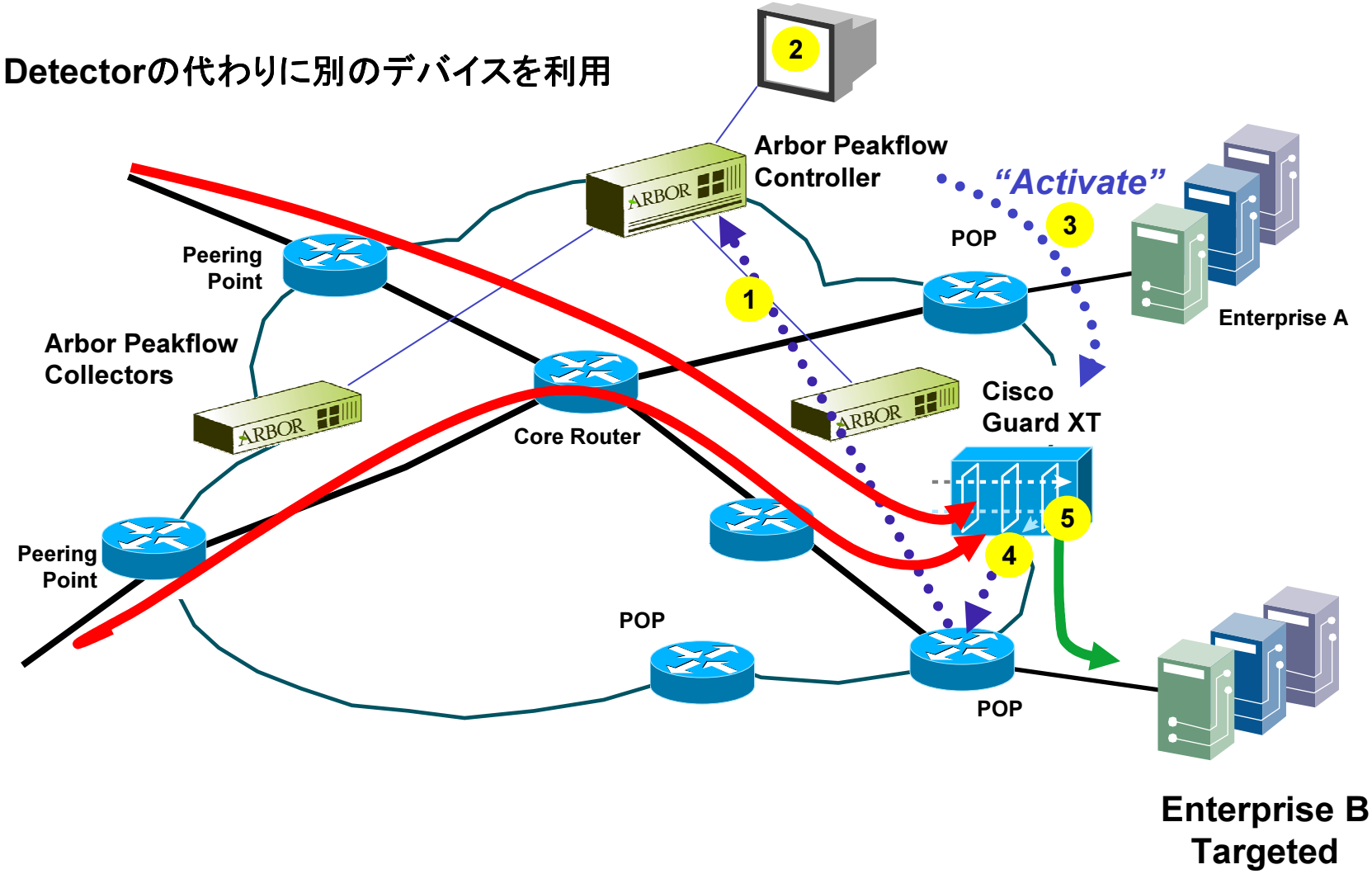
```
ip source-track 192.168.10.10
show ip source track 192.168.10.10

Address         SrcIF         Bytes   Pkts     Bytes/s     Pkts/s
192.168.10.10   Fa0/1           67M  1534K           0          0
```

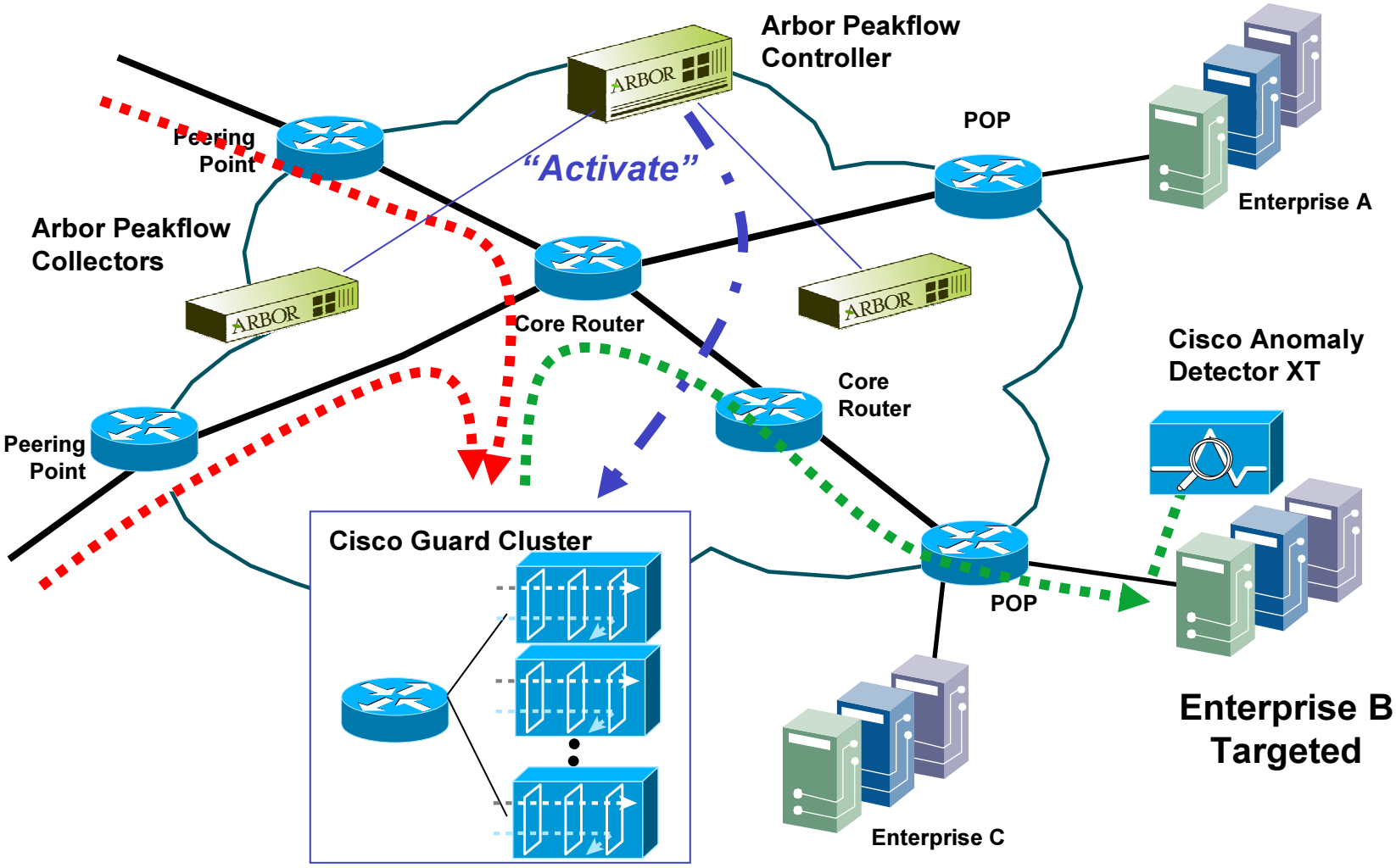
ルーターをProbeデバイスとして利用

- エッジルータからNetFlow/sFlowやらSAAのデータを取得、分析してTraffice Anomalyを検出
  - –製品として実装されてる物あり。
    - •Arbor Networks他
    - •[Anomaly Detector]の代わりに[Guard]のトリガに利用
  - –頑張ればOSSのツールだけでもやれるかも。
  - –ペイロードは見ないからスケールするし、通信の秘密にも触れずに済む？
  - –新たにProbeデバイスを撒かずに済む。
- SAA (Service Assuarance Agent)
  - –RouterからProbeのパケットを投げてRTTやサービスの生死を確認する仕組み。

Detectorの代わりにArbor Peakflowを利用



集中処理型


Arbor Peakflow
Controller
ARBOR
Peering
Point
"Activate"
POP
Enterprise A
Arbor Peakflow
Collectors
ARBOR
ARBOR
Core Router
Cisco Anomaly
Detector XT
Core
Router
Peering
Point
Cisco Guard Cluster
POP
Enterprise B
Targeted
Enterprise C

Managed Serviceの事例

DDoS Defense Option for Internet Protect managed service

- 監視サービスに対する付加機能として提供
- Arbor PeakflowとCisco Guardで構成
- 専有型、共有型をそれぞれ提供

IP Defender

- Arbor PeakflowとCisco Guardで構成
- 攻撃を検知すると顧客に通知。顧客が承認すると15分以内で緩和措置をとる。
- 専有型、共有型をそれぞれ提供

PrevenTier DDoS Mitigation Service

- Arbor PeakflowとCisco Guardで構成
- データセンターでのホスティングサービスと併せての提供
- 各種付加サービスのーメニューとして提供

Refference

- ISP Security Essentials
  http://www.getitmm.com/bootcampflash/launch.html
- [A Summay of DoS/DDoS Prevention, Monitoring and Mitigation Techniques in a Service Provicer Environment] SANS Instiute 2003
  http://www.sans.org/rr/whitepapers/intrusion/1212.php
- Cisco ISP resouce ftp://ftp-eng.cisco.com/cons/isp/security/
- Janog14「ISPにおけるDDoS対応について」
  http://www.janog.gr.jp/meeting/janog14/src/janog14_ddos_report20040721.pdf
- AT&T News Release http://www.att.com/news/2004/06/01-13096
- New World Fusion [Sprint gussying up security offerings]
  http://www.nwfusion.com/news/2004/101804-sprint.html
- Light Reading [Riverhead Protects Rackspace]
  http://www.lightreading.com/document.asp?site=lightreading&doc_id=39120