

JUNIPER TDD: 変化する脅威に対応するために 進化したDDOS攻撃対策テクニック

Juniper Networks DDoS保護ソリューション

JUNIPER
NETWORKS | Engineering
Simplicity



DDoS攻撃の影響と 現状のDDoS対策

DDOS攻撃の影響

ネットワークに求められる
現代の企業や機関にとって非常に重要な
クラウドサービスとアプリケーションの高い可用性

リスクをもたらすDDoS攻撃によるダウンタイム



DOWN

収益 統制 信頼



UP

コスト

CORERO DDOS TRENDS REPORT – 2018

2018 DDoS Trends

16%

平均攻撃数の
増加

100%

10Gbpsを超え
る攻撃数の増加

81%

10分以内に終了
する攻撃数

22%

24時間以内に同
じ犠牲者に繰り
返し攻撃される
確率

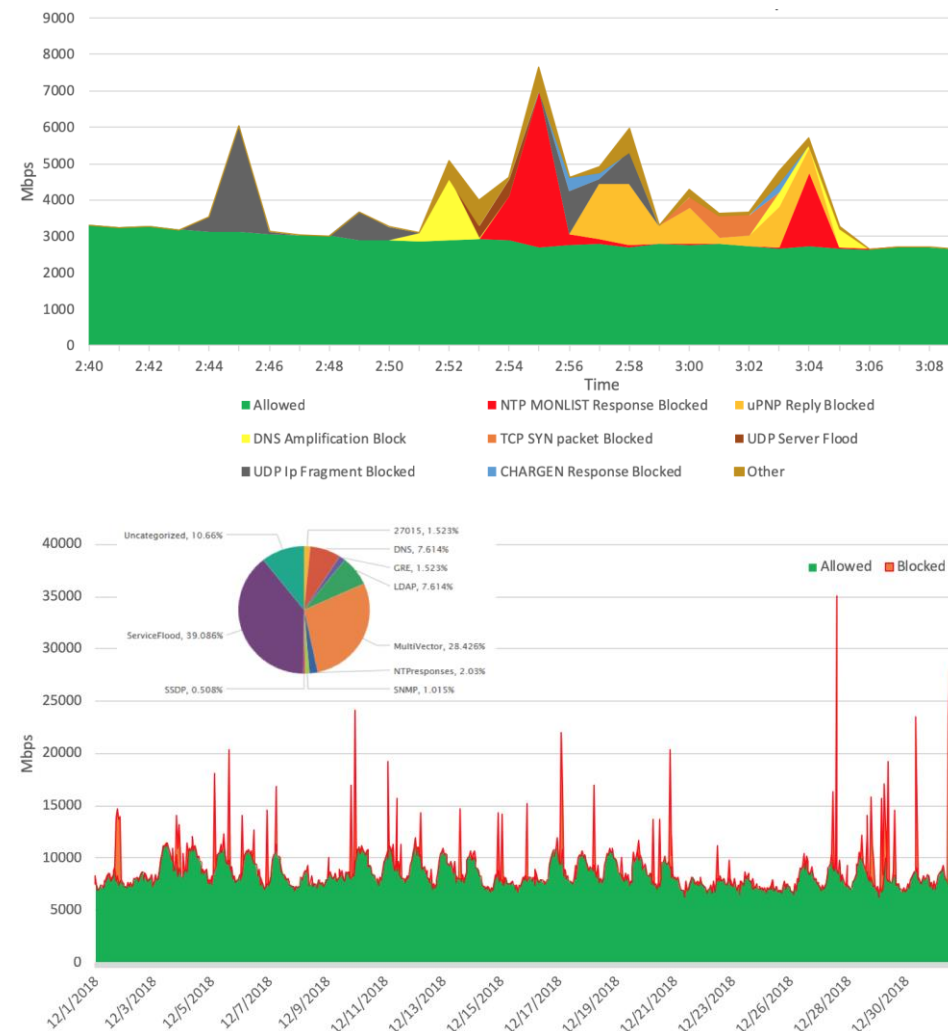
DDOS攻撃手法の進化

従来の防御を回避する攻撃

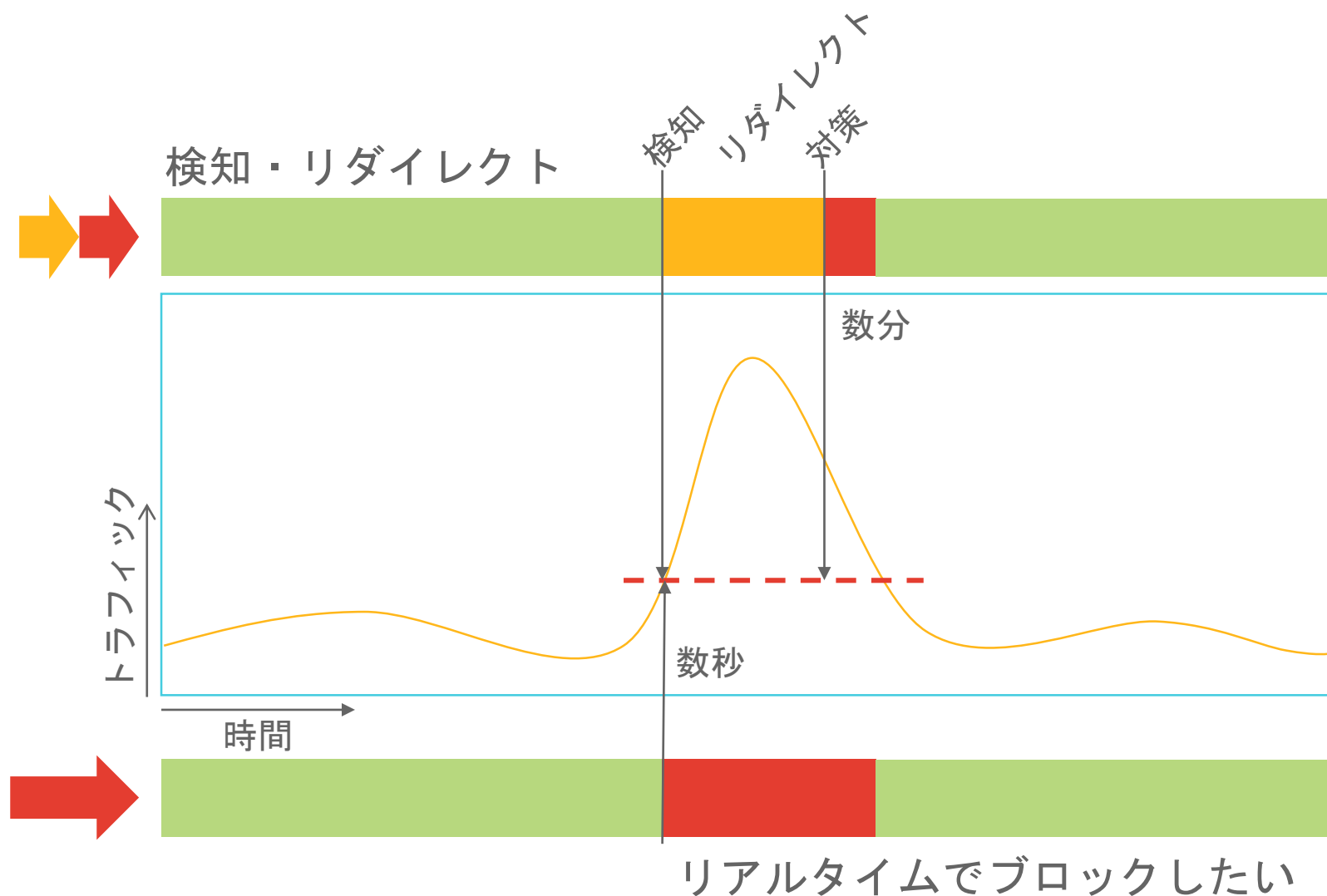
- 攻撃の長さ
- マルチベクター帯域幅の増加
- 転々とする24bitマスクプレフィックス
- 16bitプレフィックスを埋める拡散充填
- ランダム、トンネリング、なりすまし
- ホワイトノイズ
(ゾンビアタック、バックグラウンド放射)

ボットネットの再訪・改良・生まれ変わり

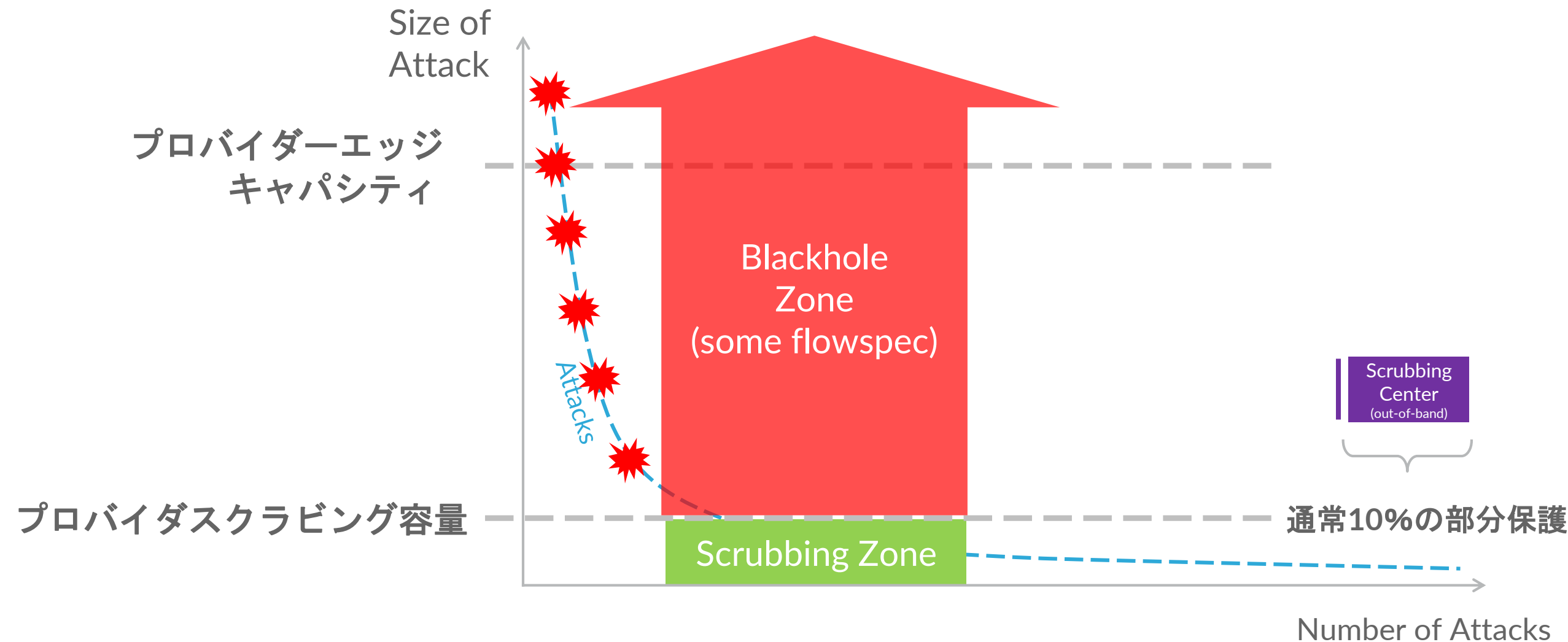
- 100,000ものメンバー
- 些細なパスワードからの所有権獲得
- 至る所で成長するIoTデバイス数（管理なし、安価）



DDOS対策までの時間



DDOS対策スタイルと攻撃規模およびエッジ容量



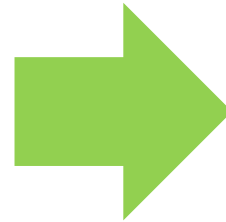


CoreroとJuniper MXによるDDoS攻撃への対策

精度の向上とDDOS検出/軽減のスピード

Netflow

- 集約遅延
- ヘッダーのみ
- 攻撃過負荷



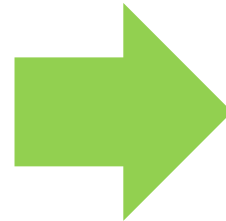
Sampled Mirror

- 即時転送
- ヘッダーとペイロード
- 攻撃を伴うスケール



Flowspec

- BGP伝播
- ヘッダーのみ
- 限られた可視性



NETCONF

- 一時的な構成
- ヘッダーとペイロード
- ストリーミングテレメトリ

NETFLOW/REDIRECTとMIRROR/NETCONF の比較

Netflow/リダイレクト

最長15分



サンプル・ミラー / Netconf

5秒未満



< 1 秒

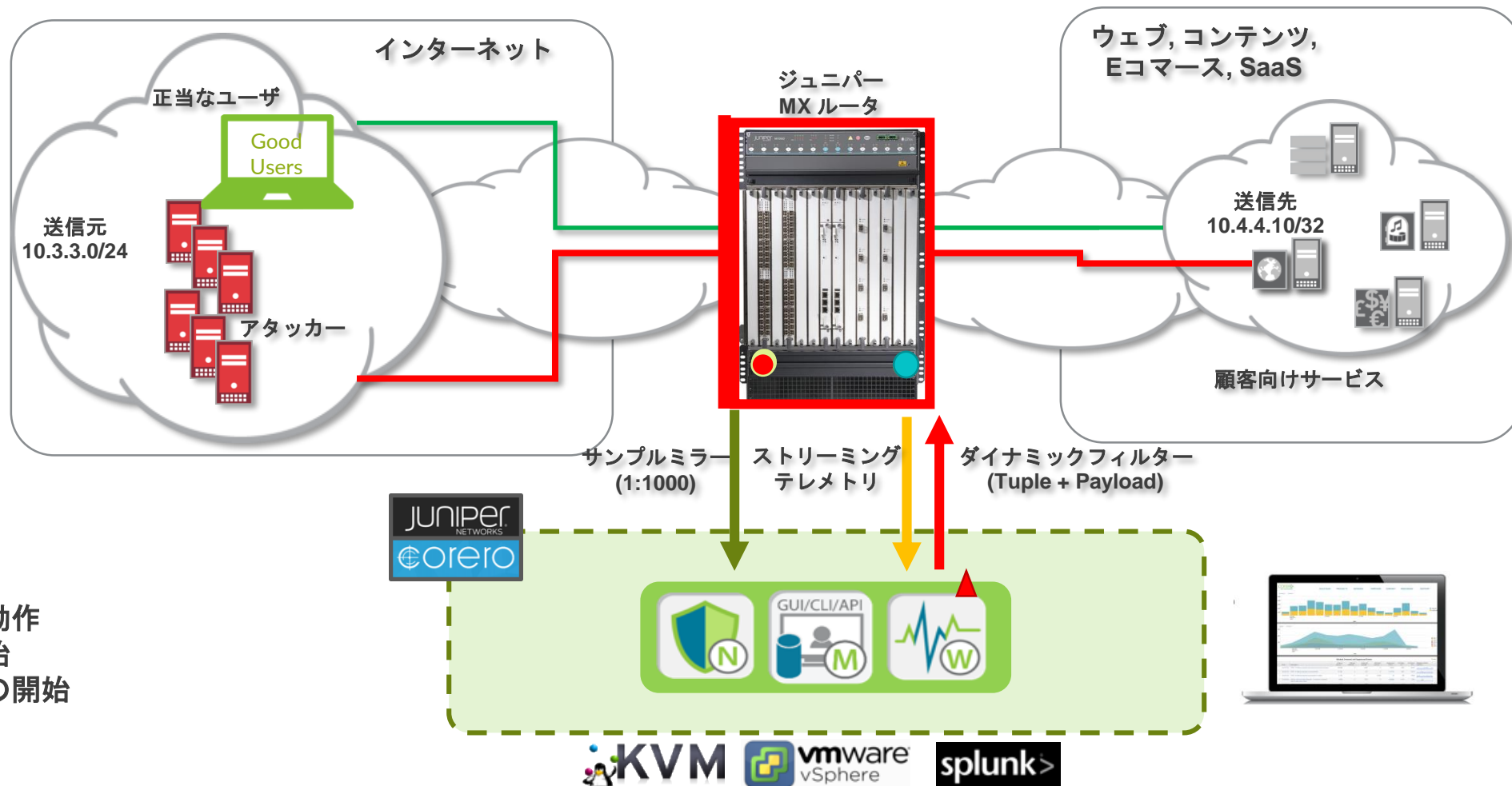
< 1 秒

< 3 秒



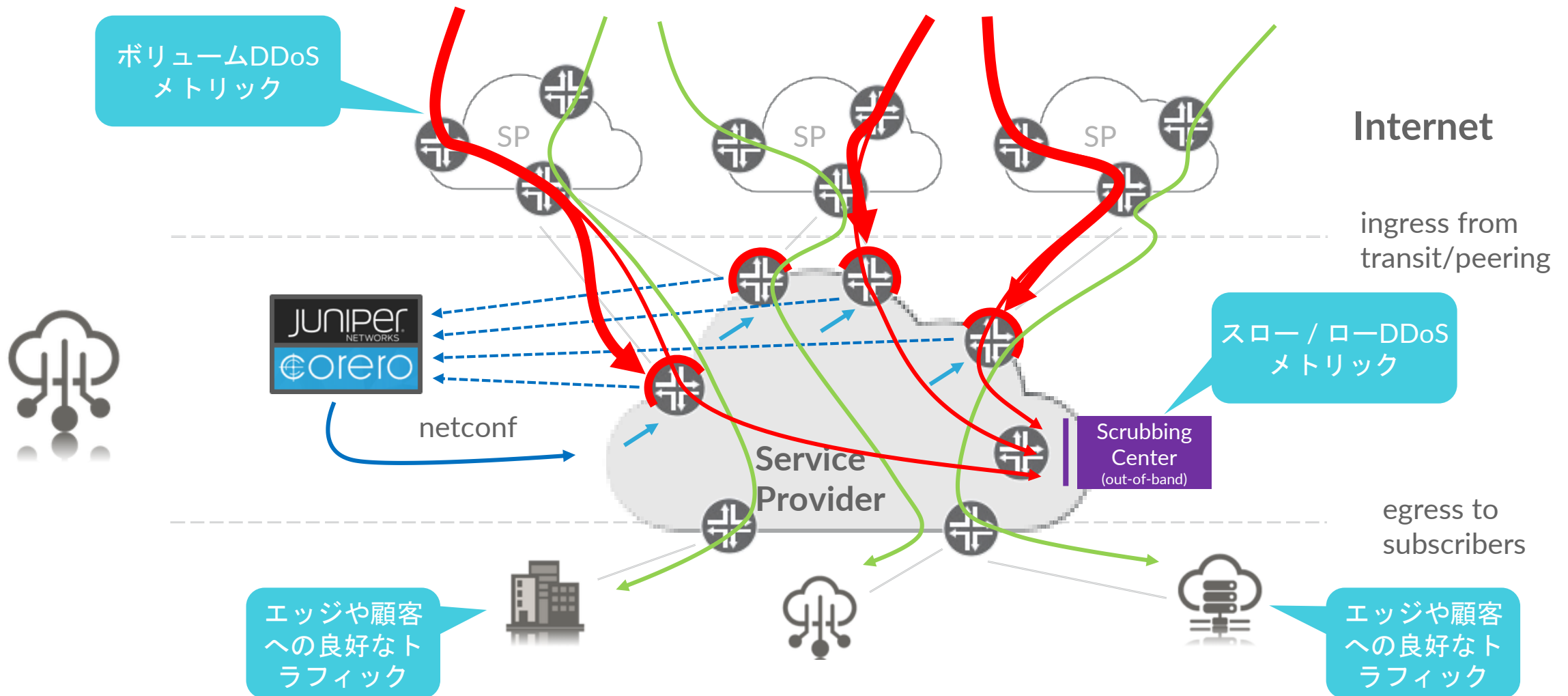
CORERO SMARTWALL TDD

DDOS検知とJUNIPER MXによる対策

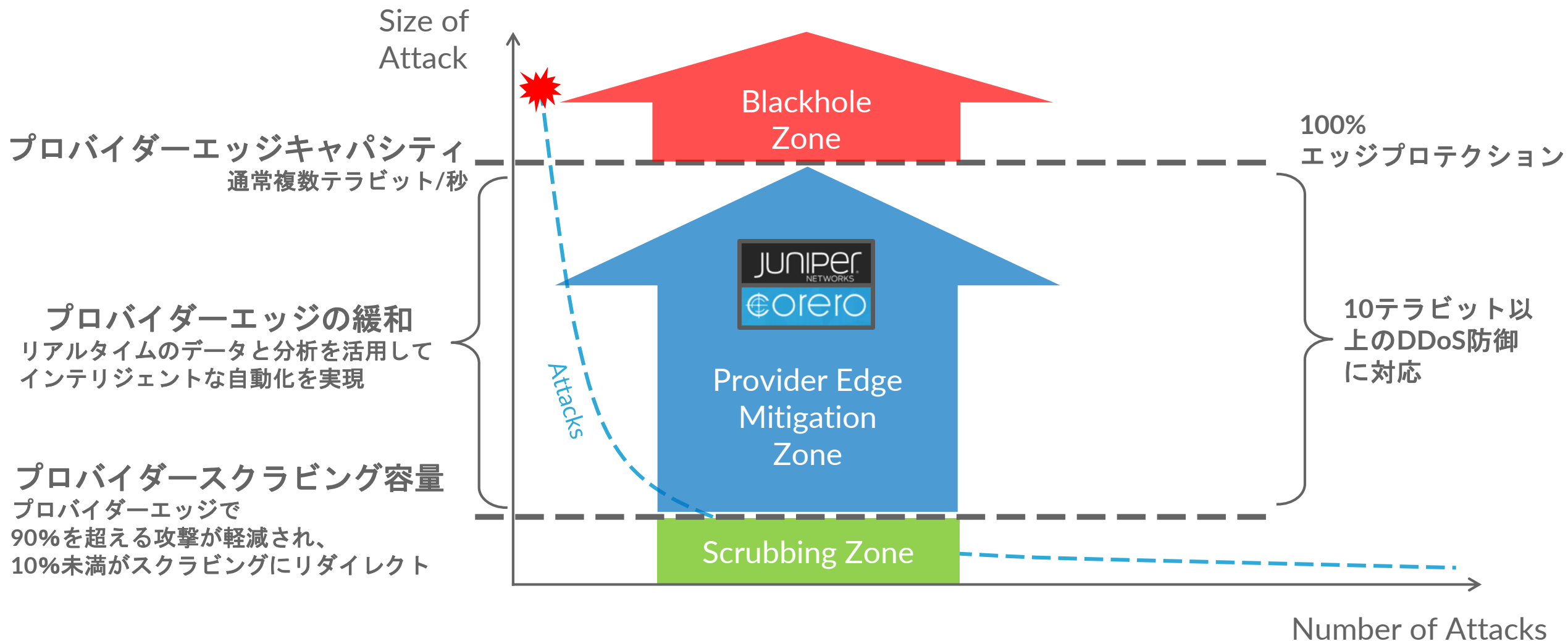


1. 正常時の動作
2. 攻撃の開始
3. 自動緩和の開始

プロバイダーエッジでの効果的なDDoS検知と対策



対策スタイルと攻撃規模およびエッジ容量



JUNIPER + COREROソリューションの利点

コスト削減

- 大量の攻撃トラフィックをスクラビングセンターに搬送するコストを削減
- 大容量スクラビングセンターの調達と維持に関連するコストを削減

顧客体験の向上

- フロー情報のエクスポートタイマーに依存しないアーキテクチャ
- 分単位から秒単位でのトラフィック削除
- 自動化
- きめ細かい攻撃トラフィックのフィルタリング
- 正当なトラフィックはフィルターされずにユーザーへ届ける

リソースの節約

- サンプルミラーリングはIPFIXと比較してルーターリソースを大幅に節約

A close-up, black and white photograph of a dandelion seed head, showing the intricate structure of the seeds and the central core. The image is used as a background for the slide.

THANK YOU

JUNIPER
NETWORKS

Engineering
Simplicity