ネットワークベースの侵入防御システム（IPS）

データセンターの資産を保護する

A Cisco on Cisco Case Study: Inside Cisco IT

概要

- 課題

  データセンターの資産を保護する

- ソリューション

  ネットワークベースの侵入防御システム（IPS）の導入

  既存の境界ベースの IPS の強化

- 成果

  データセンターへの脅威を早期に検知し緩和

課題

データセンターの資産を保護する

- シスコのネットワークに脅威がないか監視する

  内部からの脅威、データセンター資産への不正アクセス、ポリシー違反、ボットネットなど

  悪意ある行為の発生源は社の内外を問わない

- 境界ベースの IPS はネットワークの境界を通過する脅威を検知する

  シスコの DMZ やサービスプロバイダー POP に配備される

- 境界ベースの IPS はシスコのデータセンター内部のセキュリティ事象について可視性を得ることができない

  データセンター内部には会社のもっとも貴重な資産が保管されている

「2002 年の典型的な脅威は、1000 台のコンピュータから一斉に行われる 1 台のサーバを狙った攻撃でした。しかし今日では、ハッカーがデータにこっそりアクセスするのをいかに防ぐかが大きな問題です」

Cisco CSIRT チームメンバー

ソリューション

ネットワークベースの IPS の展開

- CSIRT は IPS センサーをシスコのデータセンター、エンジニアリング サーバ ルーム、オフショア開発センターに展開

  境界ベースの IPS の強化

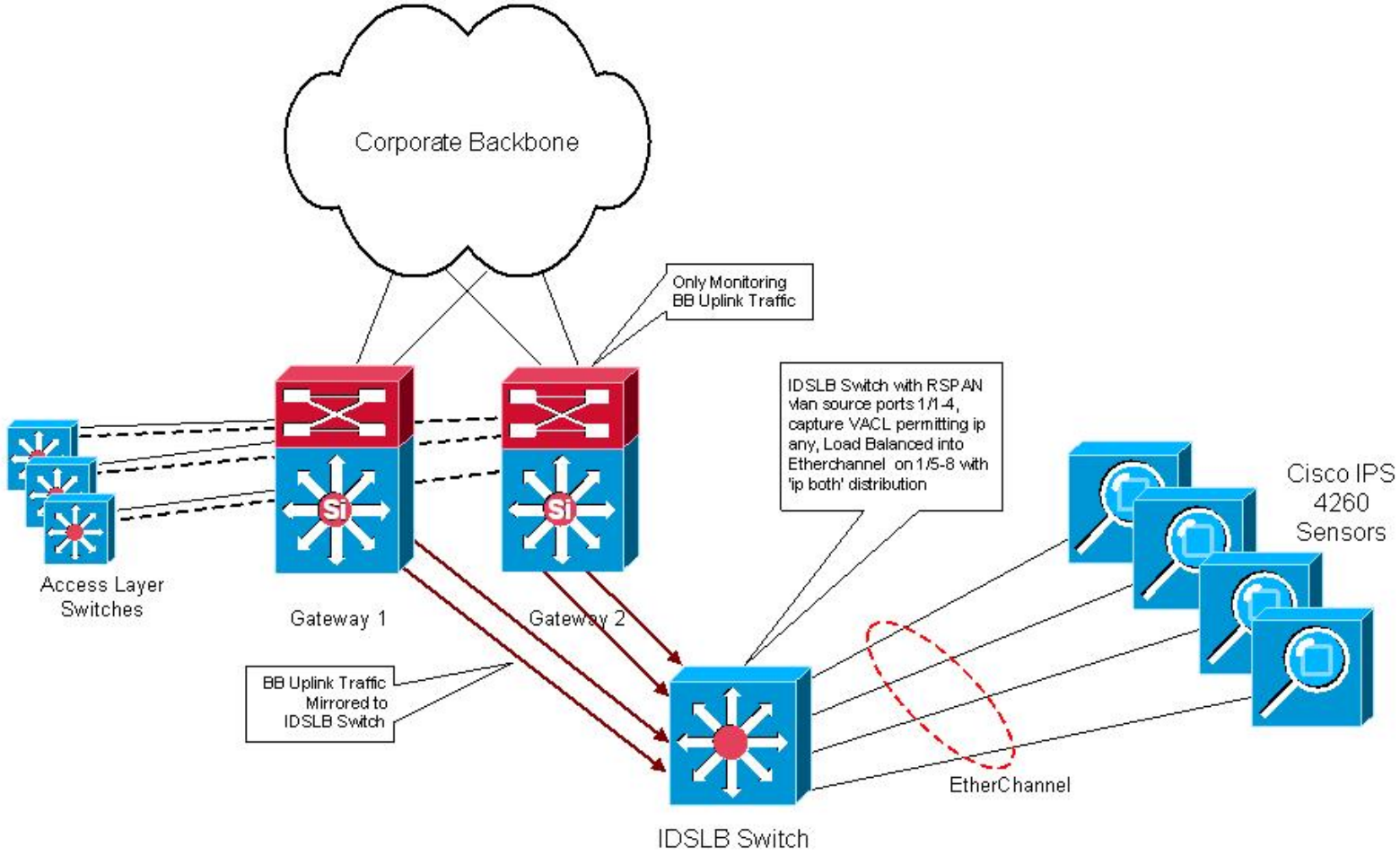
- 監視、分析、調査、センサーの調整とシグネチャのカスタマイズ、導入を伴うソリューション

  センサーの調整により、非検知を発生させずに誤検知を削減

  CSIRT はシスコのネットワーク特有の脅威に対するシグネチャのカスタマイズを継続

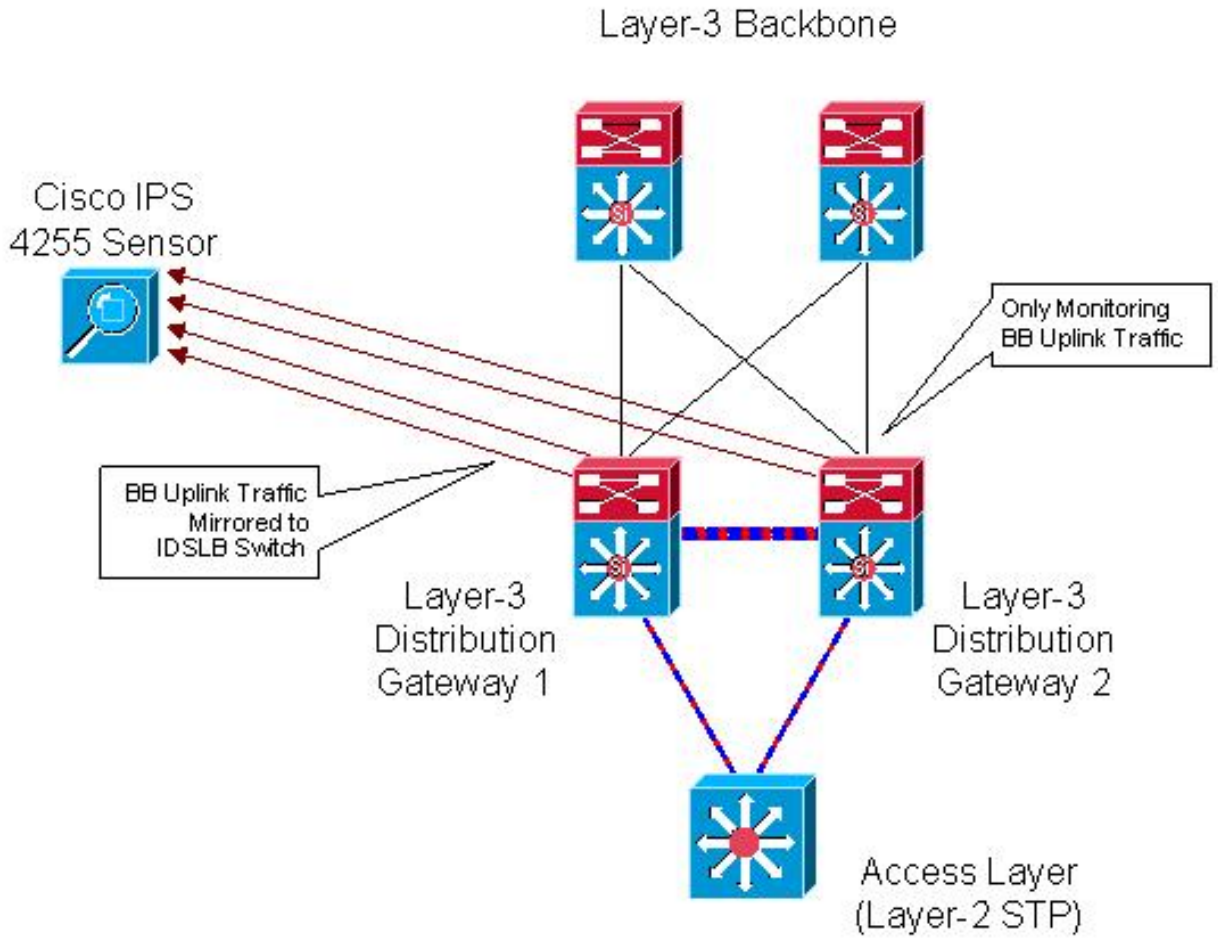
ソリューション

大規模データセンター向けの設計: 帯域幅 600 Mbps 以上



ソリューション

小規模データセンター向けの設計: 帯域幅 600 Mbps 未満



成果

データセンターに対する脅威の早期検知と緩和

- データの喪失とサービスの中断の発生を防止
- Rinbot ウィルスを発生当日に検知

  Cisco CSIRT はカスタムシグネチャを IPS に導入し、影響のあるラボシステムを特定、修復

- 2007 年 3 月から 6 月にかけて、CSIRT は毎週新しいボットネットのコマンド＆コントロールサーバを検知、影響を緩和

その他のビジネスソリューションに対するシスコ IT の事例研究は、
Cisco on Cisco ウェブサイトからご覧ください。
http://www.cisco.com/web/JP/ciscoitatwork/index.html

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**