ARBOR NETWORKS

ARBOR Pravail NSIのご紹介

Pravail NSIは、こんなお客様にお勧め

要求レベル

- ネットワーク内で、どのような通信が行われているか把握したい
- Active Directoryと連携し、ユーザ情報を付加してトラフィックを監視したい (DHCP, RADIUSとも連携)
- スマートフォンやタブレット端末(BYOD)を管理したい
- 社内リソース不正使用による情報漏洩を未然に防ぎたい
- 新しいクライアントやサーバを見つけ出しゼロデイ攻撃から守りたい
- マルウェア感染した端末からのデータ盗難を未然に防ぎたい
- ボット化した社内端末からのDDoS攻撃を未然に防ぎたい
- HTTPトラフィックに隠された不正使用による情報漏洩を未然に防ぎたい
- Webやメールからの標的型攻撃対策として既に別ベンダーの機器を導入しているがUSBメモリなどの外部記憶媒体から感染した端末を発見したい

ARBOR NETWORKS

企業における内部脅威 (情報漏洩・データ盗難、ウィルス感染など)

顧客情報漏洩で子会社の契約社員が逮捕 [redacted]

:の契約社員が顧客情報を社外へ漏洩したとして、11月29日に不正競争防止法違反容疑で愛知県警により逮捕されたことがわかった。

[redacted]のPC3台がウイルス感染 - 不正行為の告発情報など流出か

:の職員が利用するパソコン3台がウイルスに感染し、業務情報が外部へ漏洩した可能性があることがわかった。

JSSEC、消費者庁に「スマートフォン情報流出アプリ事件の対応に関する意見書」を提出

遠隔操作ウイルスによる誤認逮捕事件、犯人いまだ見つからず

POS端末を狙うマルウェア、40カ国に感染広げる

世界40カ国の小売り店やホテル、飲食店などのPOS端末が、クレジットカード情報を狙うマルウェアの標的になっているという。

日本国内にも広がるボットネットによる恐喝事件(DDoS攻撃)

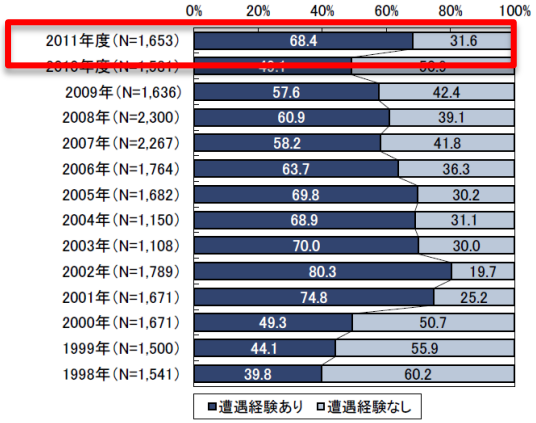
ARBOR NETWORKS

企業における内部被害

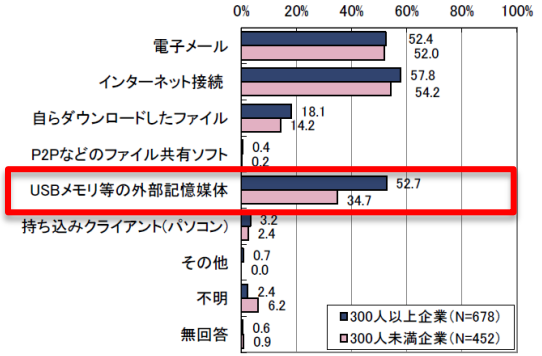
“ウィルス感染だけではなく内部者の不正使用も脅威となります”

■ウィルス感染

<ウィルス遭遇>

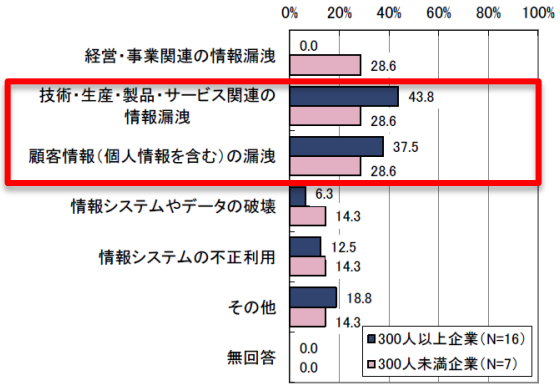


<ウィルス侵入経路>

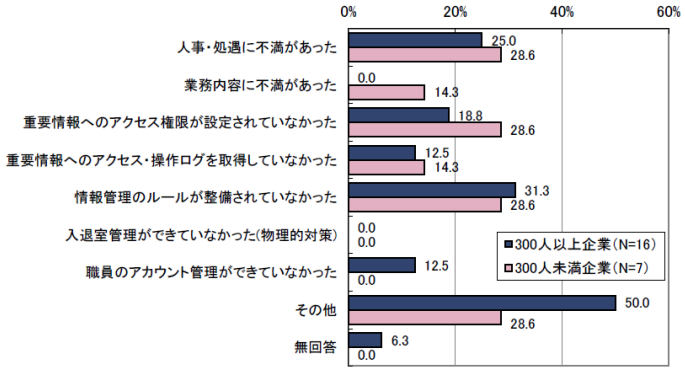


■不正使用による被害

<被害内容>



<被害が起きた原因>



※IPA:独立行政法人情報処理推進機構
「2011年度 情報セキュリティ事象被害状況調査」より

Pravail NSI 製品概要

Pravail NSI (ネットワーク・セキュリティ・インテリジェンス)

- Router・Switchから収集したxFlowやパケットデータの情報を分析し
  ネットワーク上で何が起こっているかを把握します。**（広範囲な視認性の提供）**
- トラフィックの分析結果に基づき、社内リソース不正使用に繋がる
  怪しい動きを検出します。
  （情報漏洩を未然に防止）
- 世界最大級のネットワークを解析している研究チーム(ASERT)の実績に基づく
  フィンガー・プリントにより、マルウェアに感染したホスト・
  ボット化したホストなどの異常な行動を検出します。
  （データ盗難、DDoS攻撃への加担を未然に防止）
- トラフィック分析における長年の実績をエンタープライズ向けに適用しています。
  (“Mow” ----------> “Peakflow X” ----------> “Pravail NSI”)

.0 2.0 4.0 5.0

ARBOR NETWORKS

Pravail NSI

Pravail NSI が提供する機能

1. 広範囲な視認性
ネットワーク上で何が起こっているかを知り
何を保護すべきかを発見します。

2. 身元の追跡とフォレンジックス
BYODを含む、すべてのユーザの行動を把握し、社内リソース不正使用に繋がる怪しい動きを検出し情報漏洩を未然に防止します。

3. 高度な脅威を検出
マルウェアに感染したホストからのデータ盗難・ボット化したホストのDDoS攻撃加担を未然に防止するため、異常な行動を検出します。

4. アプリケーション・インテリジェンス
アプリケーション・トラフィックを分析し新たな脅威を発見します。

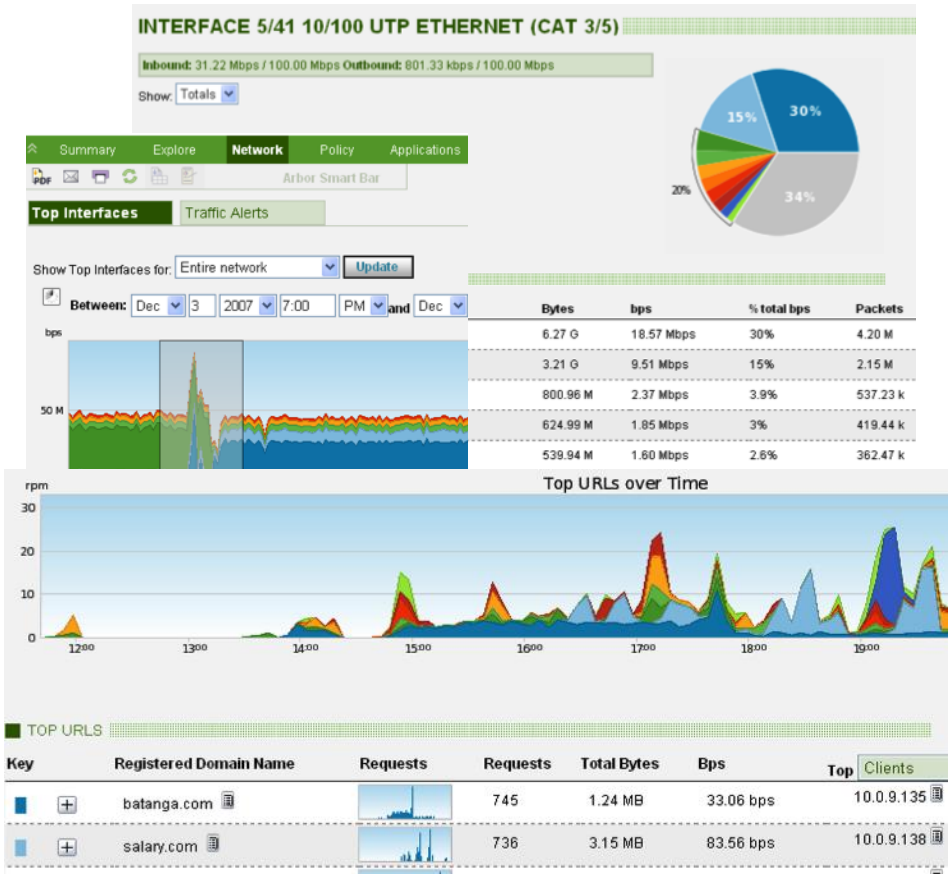
5. 優れたレポート機能
豊富なレポート・オプションによりグラフィカルなレポートを作成できます。

ARBOR NETWORKS

1. 広範囲な視認性

“ネットワーク全体を見ることができなければ、システムを保護することはできません”

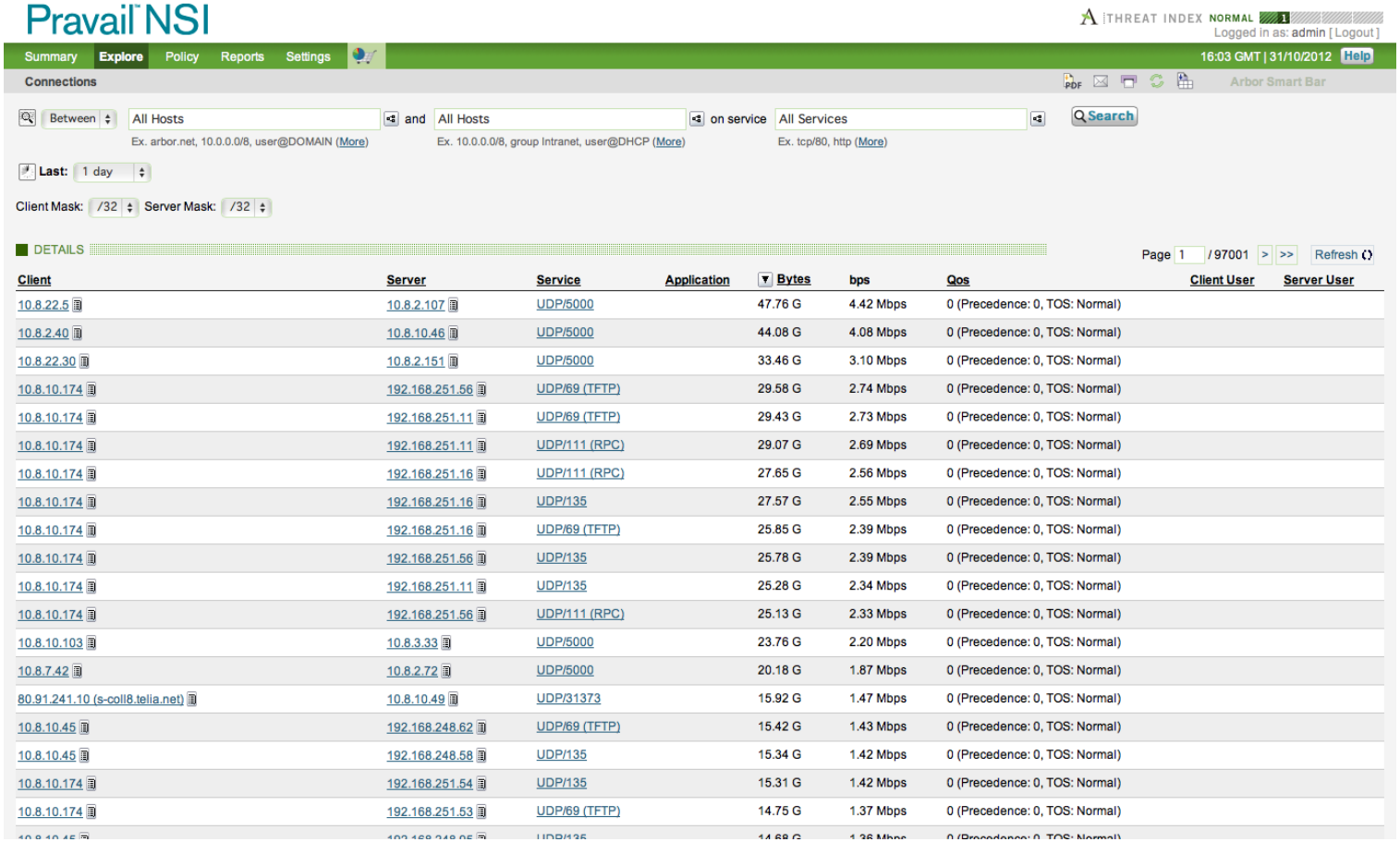
- 企業全体で費用対効果の高い可視性を得るために*Router・Switch*から収集した*xFlow (Netflow、sFlow*など)やパケットデータを活用します。
- *IPS*など境界ベースのデバイスと異なり、ネットワーク全体のトラフィック・データを取得します。



1. 広範囲な視認性 (Cont.)

Explore
Traffic
Connections
Flows
Groups, Hosts and Users
Risk Index
Routers and Interfaces
Web

- 選択したネットワーク・オブジェクト間のクライアント、サーバ、サービス、合計トラフィック・レートなど詳細なトラフィック情報を確認することが可能です。



Client	Server	Service	Application	Bytes	bps	Qos	Client User	Server User
10.8.22.5	10.8.2.107	UDP/5000		47.76 G	4.42 Mbps	0 (Precedence: 0, TOS: Normal)		
10.8.2.40	10.8.10.46	UDP/5000		44.08 G	4.08 Mbps	0 (Precedence: 0, TOS: Normal)		
10.8.22.30	10.8.2.151	UDP/5000		33.46 G	3.10 Mbps	0 (Precedence: 0, TOS: Normal)		
10.8.10.174	192.168.251.56	UDP/69 (TFTP)		29.58 G	2.74 Mbps	0 (Precedence: 0, TOS: Normal)		
10.8.10.174	192.168.251.11	UDP/69 (TFTP)		29.43 G	2.73 Mbps	0 (Precedence: 0, TOS: Normal)		
10.8.10.174	192.168.251.11	UDP/111 (RPC)		29.07 G	2.69 Mbps	0 (Precedence: 0, TOS: Normal)		
10.8.10.174	192.168.251.16	UDP/111 (RPC)		27.65 G	2.56 Mbps	0 (Precedence: 0, TOS: Normal)		
10.8.10.174	192.168.251.16	UDP/135		27.57 G	2.55 Mbps	0 (Precedence: 0, TOS: Normal)		
10.8.10.174	192.168.251.16	UDP/69 (TFTP)		25.85 G	2.39 Mbps	0 (Precedence: 0, TOS: Normal)		
10.8.10.174	192.168.251.56	UDP/135		25.78 G	2.39 Mbps	0 (Precedence: 0, TOS: Normal)		
10.8.10.174	192.168.251.11	UDP/135		25.28 G	2.34 Mbps	0 (Precedence: 0, TOS: Normal)		
10.8.10.174	192.168.251.56	UDP/111 (RPC)		25.13 G	2.33 Mbps	0 (Precedence: 0, TOS: Normal)		
10.8.10.103	10.8.3.33	UDP/5000		23.76 G	2.20 Mbps	0 (Precedence: 0, TOS: Normal)		
10.8.7.42	10.8.2.72	UDP/5000		20.18 G	1.87 Mbps	0 (Precedence: 0, TOS: Normal)		
80.91.241.10 (s-coll8.telia.net)	10.8.10.49	UDP/31373		15.92 G	1.47 Mbps	0 (Precedence: 0, TOS: Normal)		
10.8.10.45	192.168.248.62	UDP/69 (TFTP)		15.42 G	1.43 Mbps	0 (Precedence: 0, TOS: Normal)		
10.8.10.45	192.168.248.58	UDP/135		15.34 G	1.42 Mbps	0 (Precedence: 0, TOS: Normal)		
10.8.10.174	192.168.251.54	UDP/135		15.31 G	1.42 Mbps	0 (Precedence: 0, TOS: Normal)		
10.8.10.174	192.168.251.53	UDP/69 (TFTP)		14.75 G	1.37 Mbps	0 (Precedence: 0, TOS: Normal)		

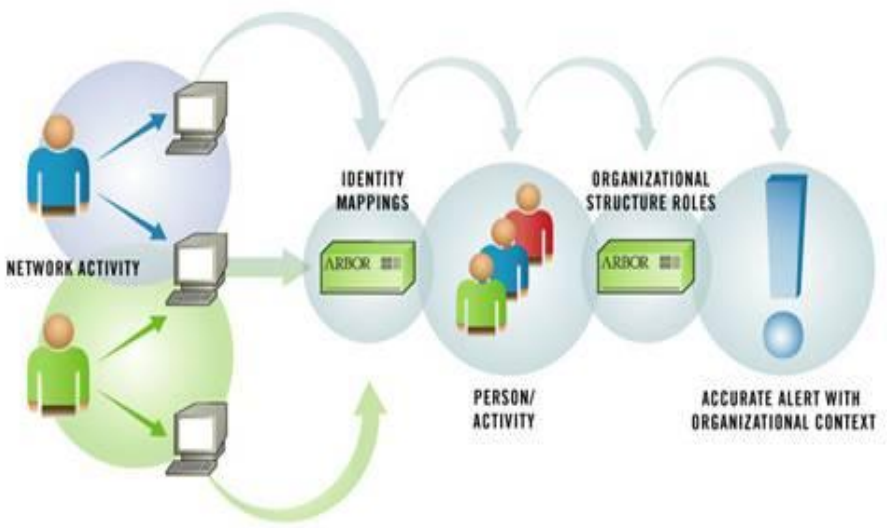
ARBOR NETWORKS

2. 身元の追跡とフォレンジックス

“BYODを含む、すべてのユーザの行動を把握し、不正使用に繋がる怪しい動きを検出することで、情報漏洩を未然に防止します”

ユーザベースのポリシーとアラート

- 身元の追跡では、どのユーザが、そのIPアドレスを使用しているかを示します。
- 個々のIPアドレスの他に身元情報を提供するためにMicrosoftのActive DirectoryやDHCPと連携します。
- RSA SecureIDなどを使用したVPN接続におけるフロントーエンドの身元追跡のためRADIUS 追跡もサポートします。



- ユーザ名・ホスト名・またはサーバからのすべての接続、サービス、およびデバイスのアクティビティにフォレンジックスを活用します。

“活動ベース”の検出 (リスク・スコア計算)

- リスクスコアは、Pravail NSIのセキュリティ・ポリシーによって計算され、スコアの高いものから表示されます。

RISK INDEX

Page 1 / 1 Refresh

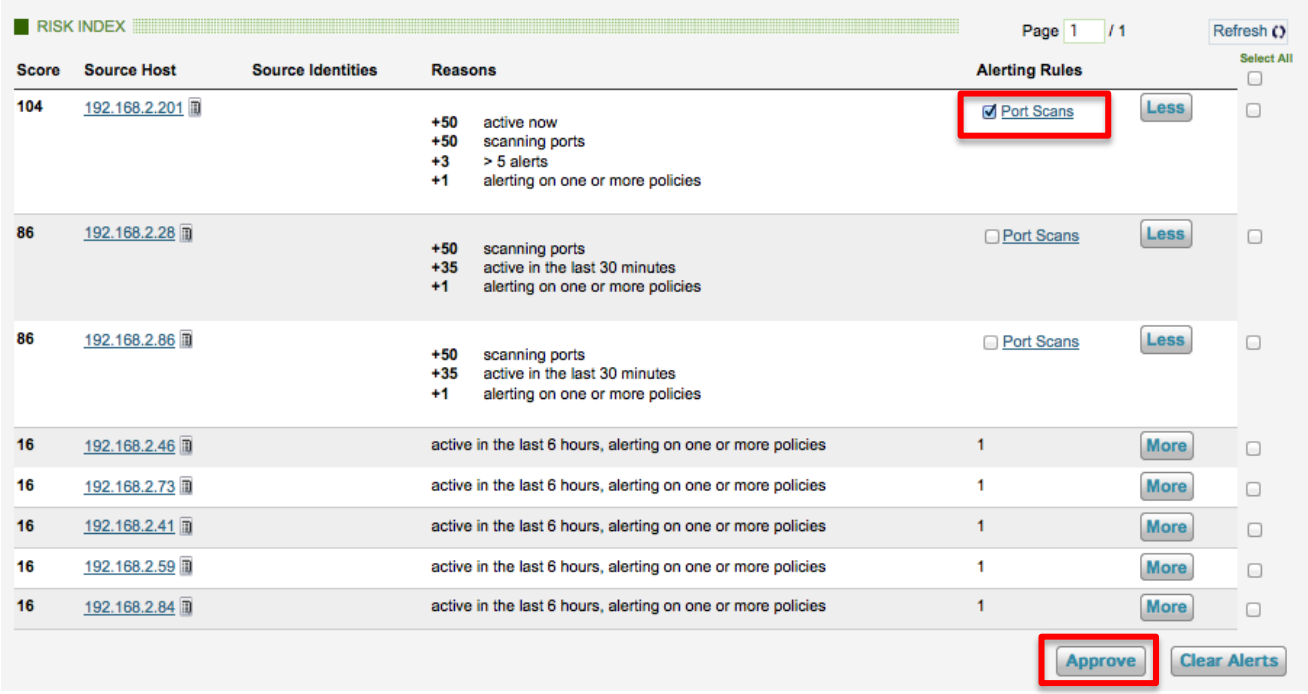
Score	Source Host	Source Identities	Reasons	Alerting Rules	
104	192.168.2.201		+50 active now +50 scanning ports +3 > 5 alerts +1 alerting on one or more policies	Port Scans	Less
86	192.168.2.28		+50 scanning ports +35 active in the last 30 minutes +1 alerting on one or more policies	Port Scans	Less
86	192.168.2.86		+50 scanning ports +35 active in the last 30 minutes +1 alerting on one or more policies	Port Scans	Less
16	192.168.2.46		active in the last 6 hours, alerting on one or more policies	1	More
16	192.168.2.73		active in the last 6 hours, alerting on one or more policies	1	More
16	192.168.2.41		active in the last 6 hours, alerting on one or more policies	1	More
16	192.168.2.59		active in the last 6 hours, alerting on one or more policies	1	More
16	192.168.2.84		active in the last 6 hours, alerting on one or more policies	1	More

Select All

Approve Clear Alerts

“活動ベース”の検出 (ホワイト・リスト化)

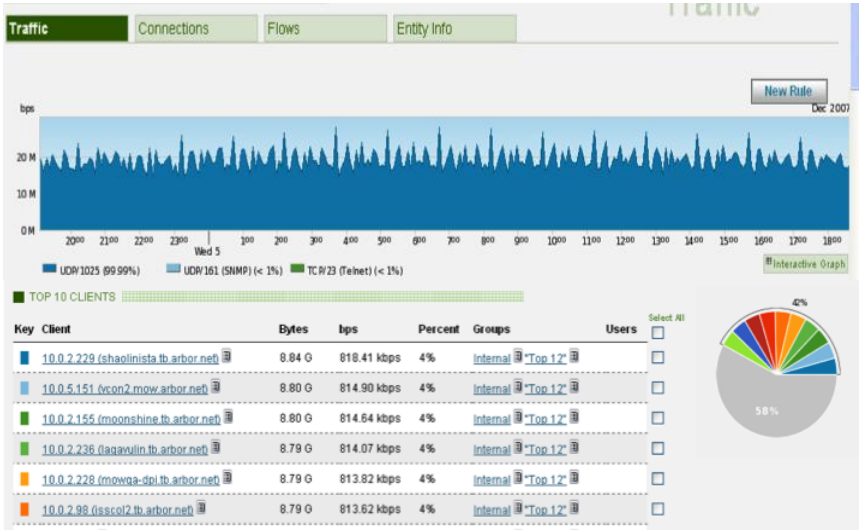
- ホスト(192.168.2.201)は、IT部門が使用するワークステーションで
  セキュリティ・テストのためにポート・スキャンをしている場合など
  セキュリティ上、問題がないと判断したものに関してはホワイト・リスト化
  することで、このアラームを無視することができます。



3. 高度な脅威を検出

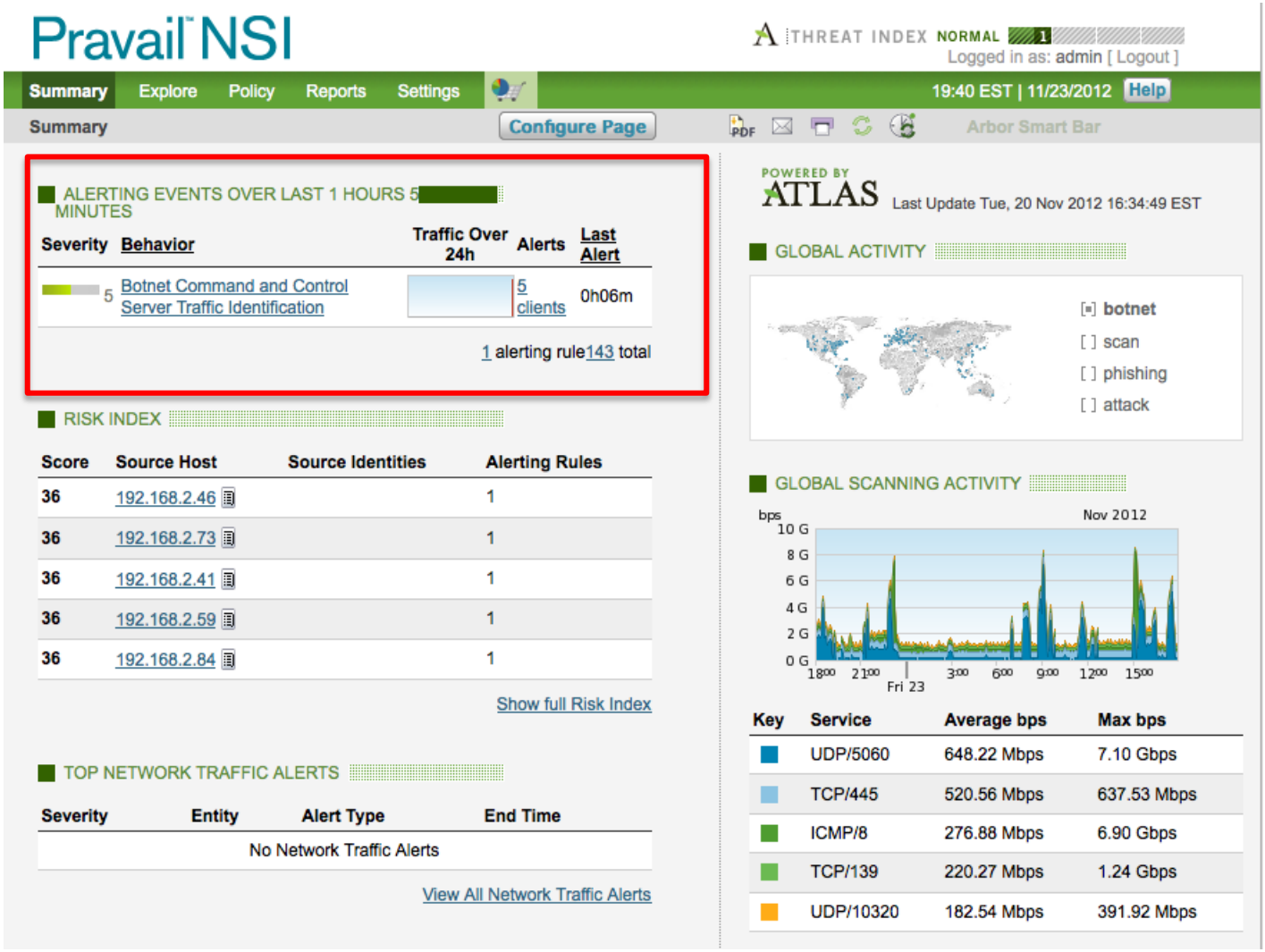
“マルウェアに感染したホストからのデータ盗難・ボット化したホストのDDoS攻撃加担を未然に防止します”

- 世界最大級のネットワークを解析している研究チーム(ASERT)の実績に基づいたフィンガー・プリント(ATF)を活用します。
- マルウェアに感染したホストの異常な行動を検出します。
- ボット化したホストとボット・ハーダー(C&C)の通信を検出します。

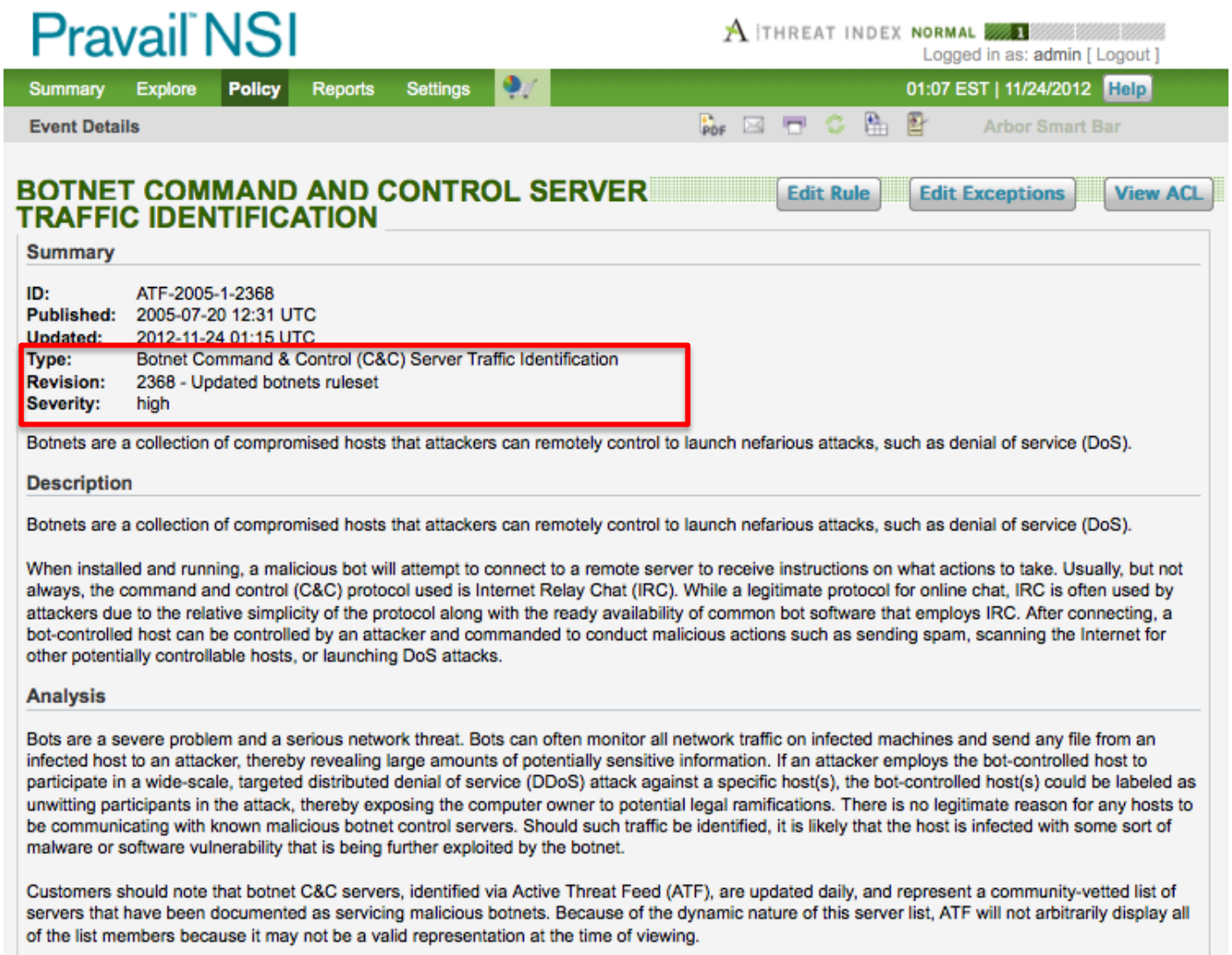


ARBOR NETWORKS

“振る舞いベース”の検出 (ボットネットの発見)



“振る舞いベース”の検出 (ボットネットの発見)



“振る舞いベース”の検出 (ボットネットの発見)

- 発見した脅威に対して、どのような対処をすべきか情報を提供します。

Affected Platforms and Versions

Any Internet-connected host running Windows, Linux, and/or Unix could potentially be affected. Malicious bots usually propagate automatically, scanning for unpatched vulnerabilities in popular network software and exploiting them to install malicious code on a host without the owner's knowledge. Alternatively, bots can propagate like a traditional Trojan horse or virus, tricking users into running malicious code, e.g., an e-mail that contains a deceivingly named attachment.

Remediation

If possible, remove infected hosts from the network, scan for any installed malware, and ensure that all the latest and most relevant patchsets are installed.

Workaround

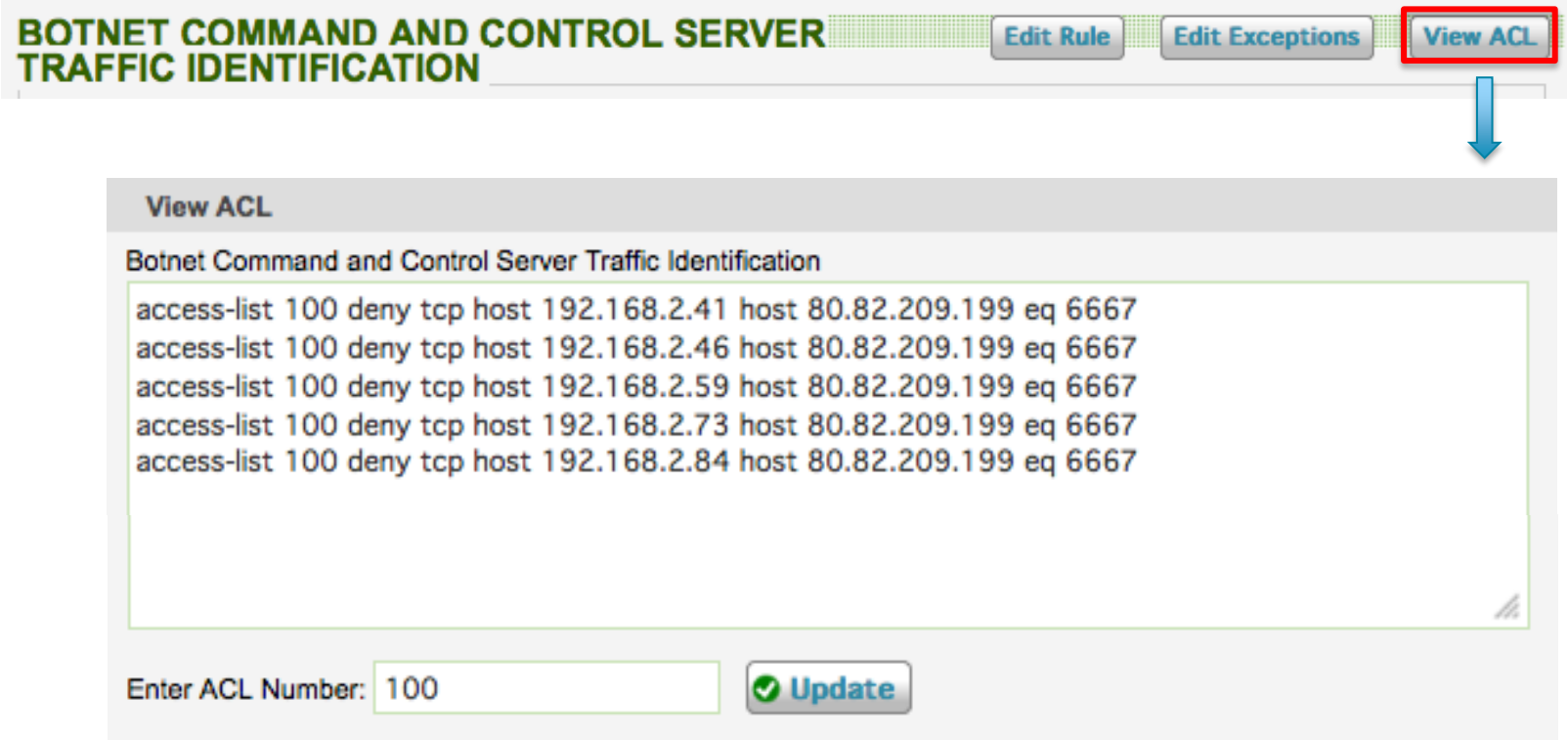
Consider blocking common IRC ports, such as TCP ports 6667-6669. Customers should note that many botnet control servers are accessed via non-standard ports in order to evade detection. For a more robust workaround, deploy an application-aware firewall to block bilateral IRC network traffic. This prevents some bots from communicating with their C&C botnet server(s).

General References

Date	Organization	Author	E-mail Address	Title
2005-11-08	Wikipedia			Botnet
2005-12-01	CERT/CC	Nicholas Ianelli, Aaron Hackworth		Botnets as a Vehicle for Online Crime
2005-03-13	The Honeynet Project & Research Alliance			Know your Enemy: Tracking Botnets
2005-10-17	National Infrastructure Security Co-ordination Centre			Botnets - the threat to the Critical National Infrastructure
2007-07-06	Shadowserver			Shadowserver Foundation - Information - Botnets

“振る舞いベース”の検出 (ボットネットの発見)

- Pravail NSI はホストからマルウェアを除去している間、
  C&Cからのトラフィックをブロックするための**ACL**設定例を生成できます。



“振る舞いベース”の検出 (フィンガープリント)

“世界トップクラスのフィンガープリントにより高度な脅威を検出します”

Tier1サービスプロバイダの**90%**を
お客様として抱えるARBORは日々、
新たな脅威を分析するワールド・クラスの
研究チーム(ASERT)によって世界トップクラスの
“フィンガープリント” を生み出します。

– 既知または新たな脅威に対する
詳細なトラフィック・パターンを活用します。

“フィンガープリント”は**Active Threat Feed (ATF)**としてPravail NSIをご使用される
お客様に提供されます。

“振る舞いベース”の検出 (世界トップクラスの研究)

“高度な脅威の識別・分析に特化したワールド・クラスの研究チーム(*ASERT*)がフィンガープリント(*ATF*)を提供します”

識別

ネットワークの脅威を
識別・分析するために
世界中のインフラを監視。
(Tier1サービスプロバイダの**90%**がARBORのお客様)

ATLAS

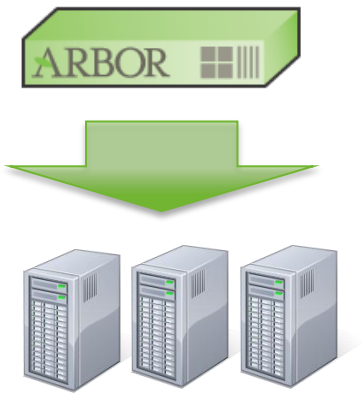
マルウェア
ボットネット
フィッシング
P2P

分析

ASERT

フィンガープリント

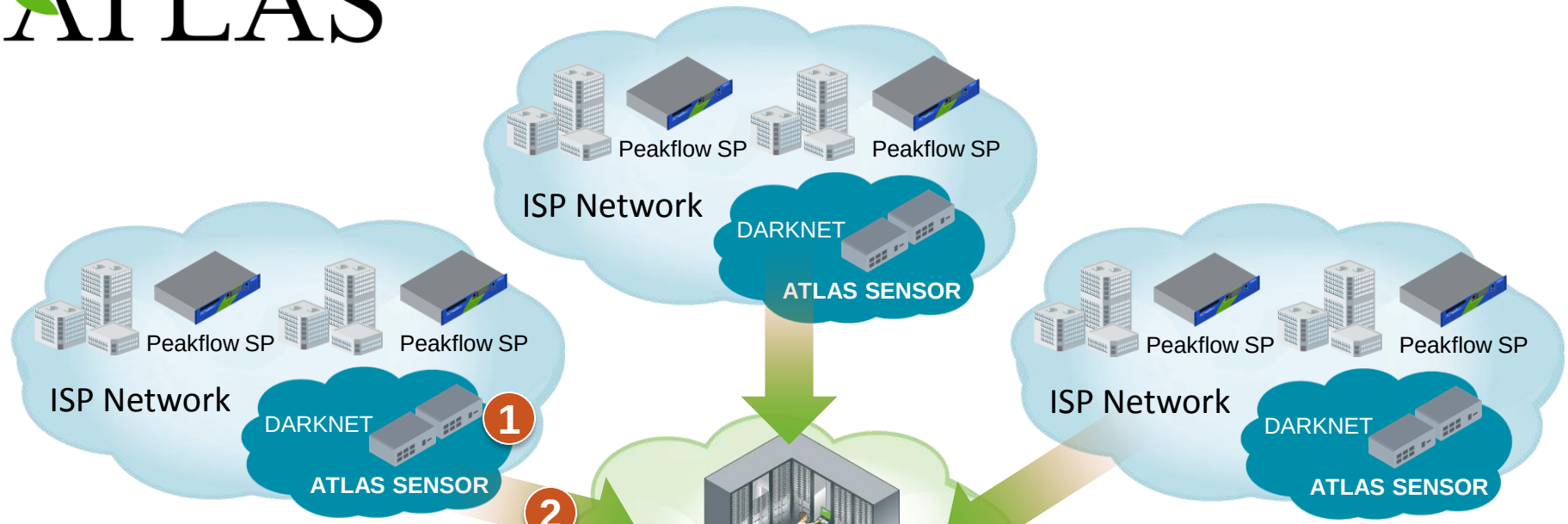
保護



ARBOR NETWORKS

ATLAS (Active Threat Level Analysis System)

ATLAS®



❶ 攻撃活動を発見し分類するためにダークネット空間でATLAS SENSORが展開される。

❷ ARBORのPeakflow、サードパーティおよび脆弱性のデータと組み合わせてATLAS DATA CENTERに送信される。

❸ 研究チーム(ASERT)は、そのデータを結合し分析した結果をポータル・サイトに公開する。
・過去24時間の攻撃種類トップ
・過去24時間の攻撃における送信元など

http://atlas.arbor.net/

ARBOR NETWORKS

アラート通知

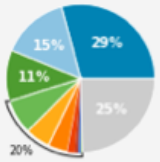
“Pravail NSI はネットワークの内部に存在する様々な脅威を検出し警告します”

- ポート & ホスト スキャン
- ボットネット
- マルウェア
- スパイウェア
- ダークIP検出 (未使用IP空間)
- 不正アクセス

- 新しいクライアント
- 新しいサーバ
- 新しいサービス
- ホスト間の新しい関係性

ALERT SUMMARY

Key	Rule	Alert Count
	Unauthorized SSH servers	314
	Rapidshare Traffic Identification	158
	Worm.Downanup Variants	120
	Privax Proxy Network	81
	US Embargoed Nation(s) Traffic Identification: Libya	58
	Botnet Command and Control Server Traffic Identification	46
	US Embargoed Nation(s) Traffic Identification: Myanmar	17
	Port Scans	8
	US Embargoed Nation(s) Traffic Identification: Cuba	6
	Dark IP Traffic	3
	Trojan.Sinowal Variants	3
	US Embargoed Nation(s) Traffic Identification: North Korea	2
	Atrivo Network Traffic	2
	ICMP ping flood to 213.85.31.7	1
	ICMP ping flood to 213.85.31.14	1



ARBOR NETWORKS

アラート通知 (Cont.)

“E-mail・Syslog・SNMP Trapにより、アラートを通知します”

Pravail NSI

THREAT INDEX NORMAL 1

Logged in as: admin [Logout]

Summary | Explore | Policy | Reports | Settings | 2 new | 0 queued | 20:27 GMT | 30/10/2012 | Help

View Report | Arbor Smart Bar

REPORT 11 : ALERT SUMMARY REPORT

30 Oct 2012 19:18 to 30 Oct 2012 19:33 (15 Minutes)

Save or Schedule

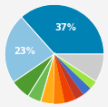
Report Description

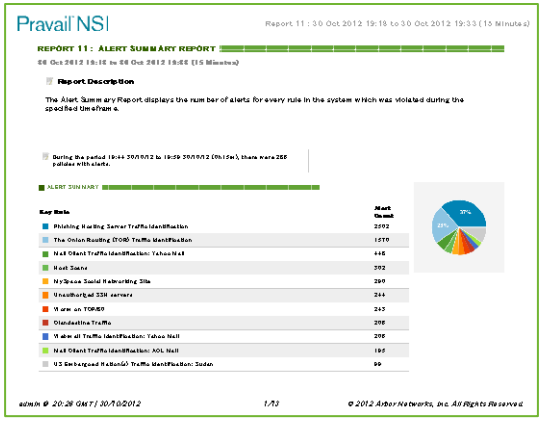
The Alert Summary Report displays the number of alerts for every rule in the system which was violated during the specified timeframe.

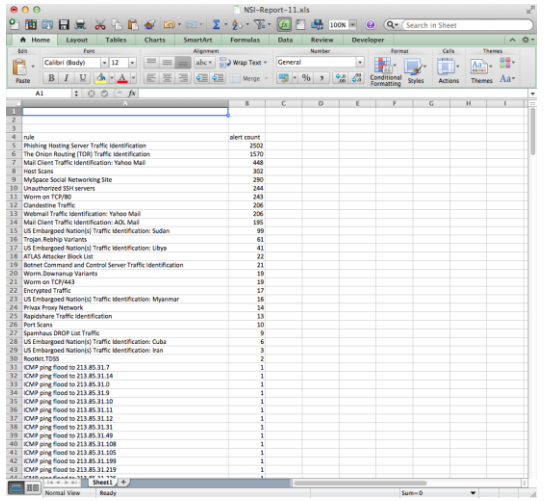
During the period 19:44 30/10/12 to 19:59 30/10/12 (0h15m), there were 286 policies with alerts.

ALERT SUMMARY

Key	Rule	Alert Count
	Phishing Hosting Server Traffic Identification	2502
	The Onion Routing (TOR) Traffic Identification	1570
	Mail Client Traffic Identification: Yahoo Mail	448
	Host Scans	302
	MySpace Social Networking Site	290
	Unauthorized SSH servers	244
	Worm on TCP/80	243
	Clandestine Traffic	206
	Webmail Traffic Identification: Yahoo Mail	206
	Mail Client Traffic Identification: AOL Mail	195
	US Embargoed Nation(s) Traffic Identification: Sudan	99
	Trojan.Rebhip Variants	61
	US Embargoed Nation(s) Traffic Identification: Libya	41
	ATLAS Attacker Block List	22
	Botnet Command and Control Server Traffic Identification	21
	Worm.Downanup Variants	19
	Worm on TCP/443	19



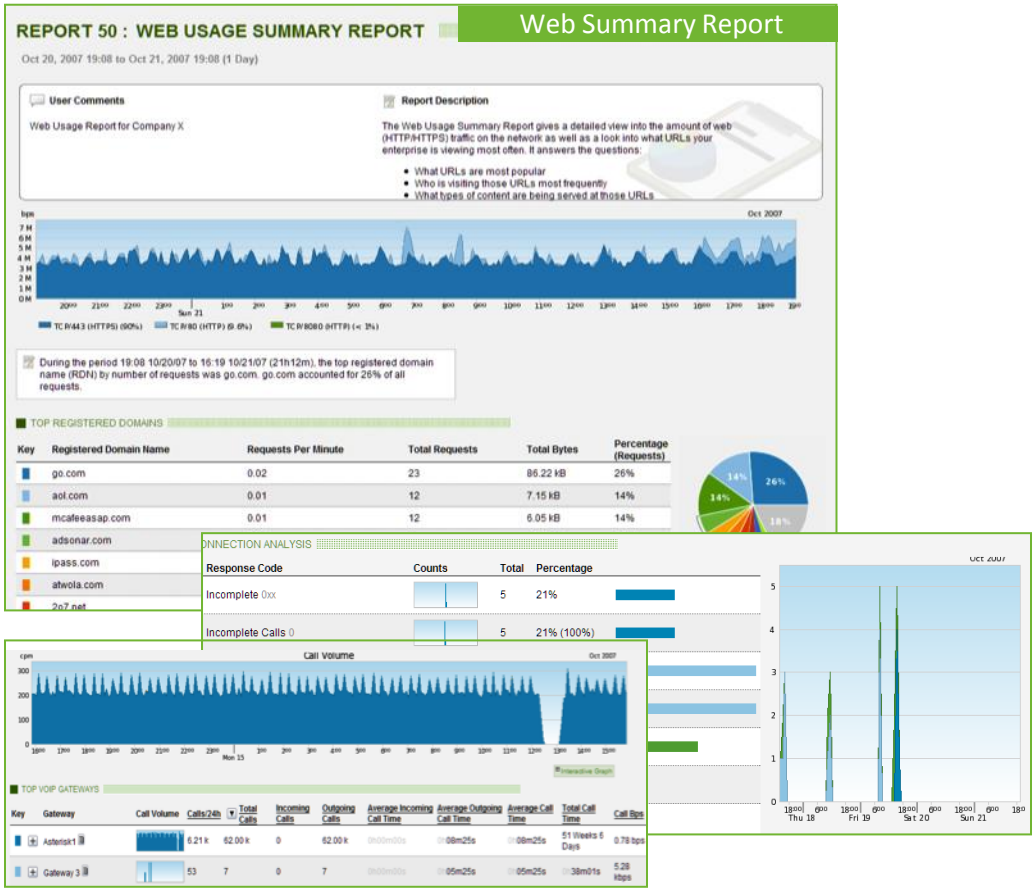




ARBOR NETWORKS

4. アプリケーション・インテリジェンス

“アプリケーション・トラフィックを分析し 新たな脅威を検出します”



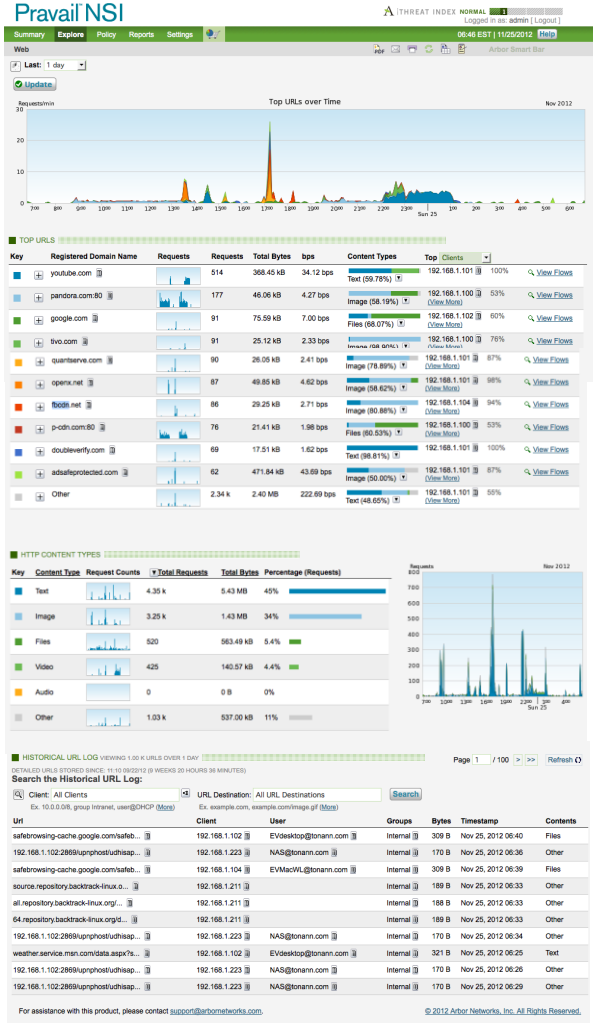
- *HTTP*トラフィックに隠された不正使用による情報漏洩を未然に防ぎます。
- *URL*の利用、把握していないトラフィック、データ転送タイプのレポートによって情報漏洩を未然に防止します。(P2P、インスタント・メッセージ)
- 誰が、どのような*Web*サイトを開きどのようなアプリケーションを使用しているかを把握します。

ARBOR NETWORKS

4. アプリケーション・インテリジェンス (Cont.)

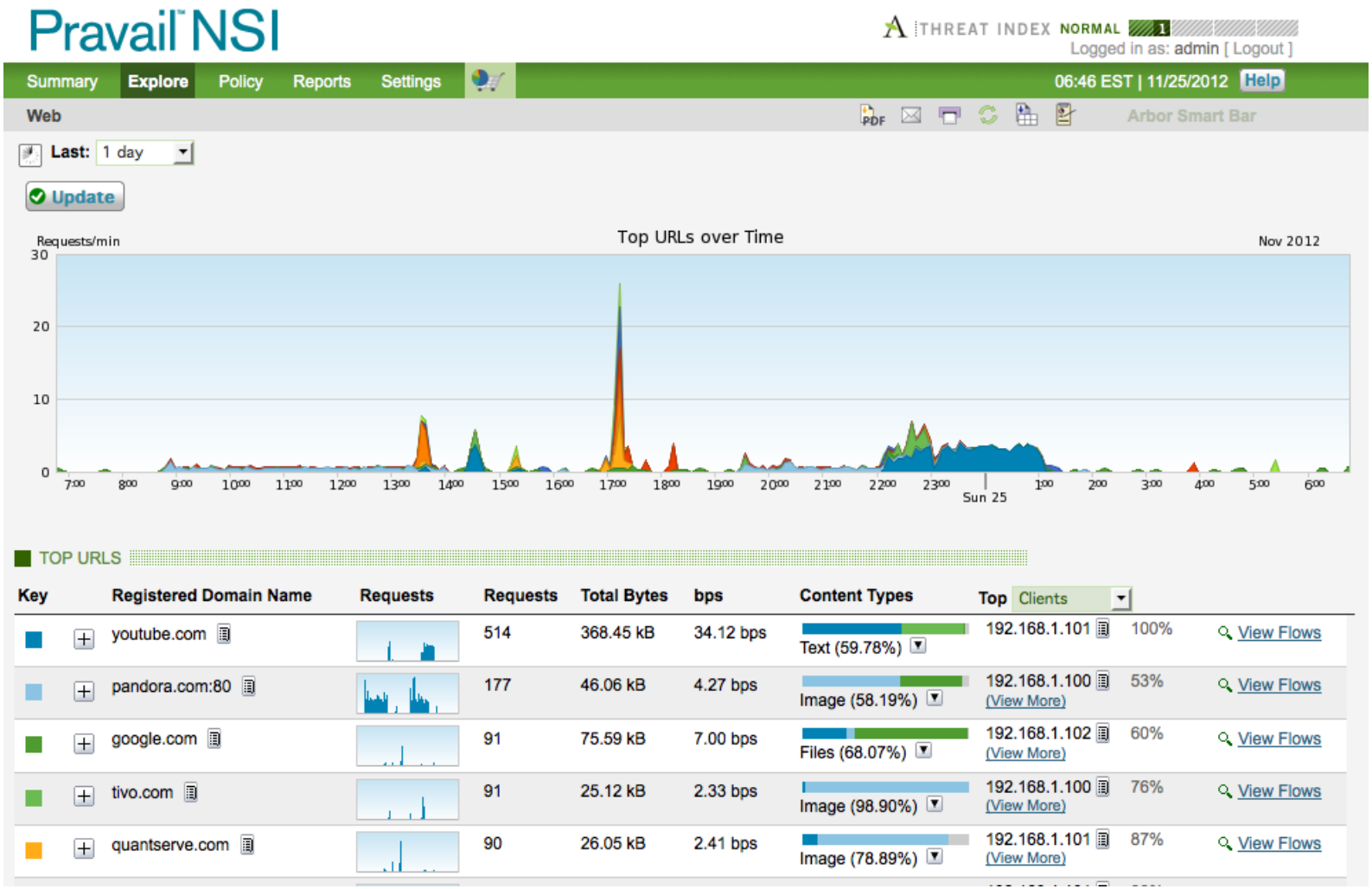
Explore
Traffic
Connections
Flows
Groups, Hosts and Users
Risk Index
Routers and Interfaces
Web

“HTTPトラフィックに隠された不正使用を追跡します”



- Pravail NSI AIコレクタを使用して頻繁にアクセスされるWebアプリケーションを識別し、追跡します。
  - トップURL
  - HTTP コンテンツ・タイプ
  - URL ログ

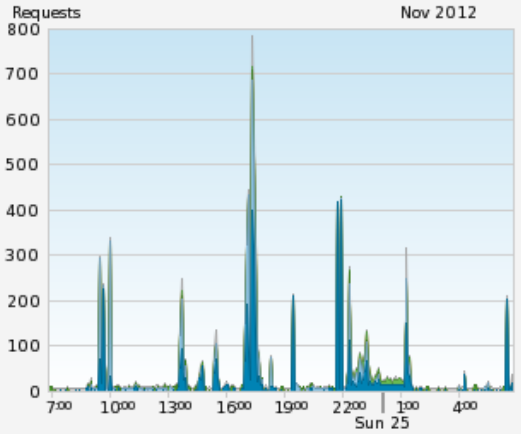
トップURL


Pravail NSI
THREAT INDEX NORMAL 1
Logged in as: admin [Logout]
Summary
Explore
Policy
Reports
Settings
06:46 EST | 11/25/2012
Help
Web
Arbor Smart Bar
Last: 1 day
Update
Top URLs over Time
Requests/min
Nov 2012
Sun 25
TOP URLS
Key
Registered Domain Name
Requests
Requests
Total Bytes
bps
Content Types
Top Clients
youtube.com 514 368.45 kB 34.12 bps Text (59.78%) 192.168.1.101 100% View Flows
pandora.com:80 177 46.06 kB 4.27 bps Image (58.19%) 192.168.1.100 (View More) 53% View Flows
google.com 91 75.59 kB 7.00 bps Files (68.07%) 192.168.1.102 (View More) 60% View Flows
tivo.com 91 25.12 kB 2.33 bps Image (98.90%) 192.168.1.100 (View More) 76% View Flows
quantserve.com 90 26.05 kB 2.41 bps Image (78.89%) 192.168.1.101 (View More) 87% View Flows

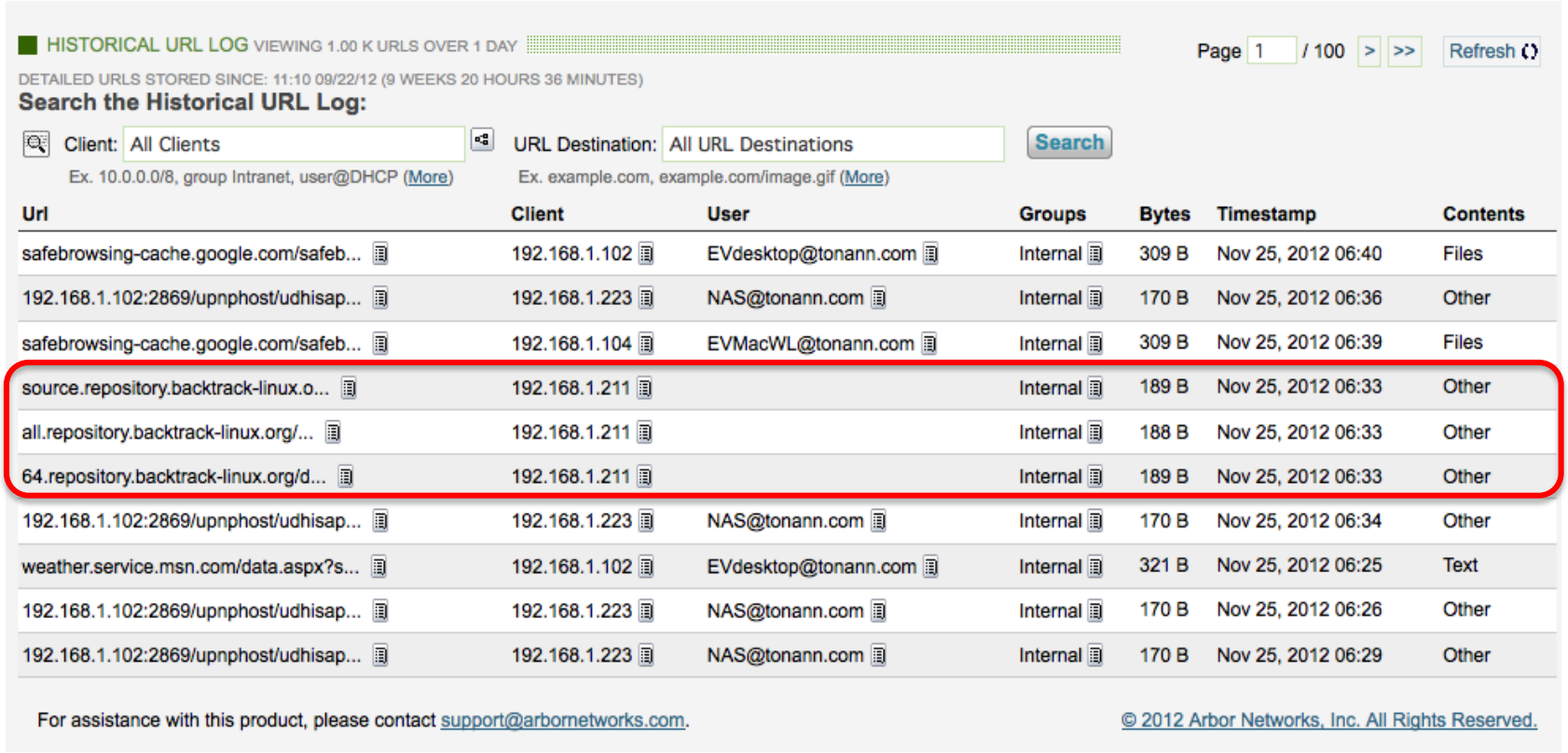
HTTP コンテンツ・タイプ

HTTP CONTENT TYPES

Key	Content Type	Request Counts	Total Requests	Total Bytes	Percentage (Requests)
	Text		4.35 k	5.43 MB	45%
	Image		3.25 k	1.43 MB	34%
	Files		520	563.49 kB	5.4%
	Video		425	140.57 kB	4.4%
	Audio		0	0 B	0%
	Other		1.03 k	537.00 kB	11%



URL ログ



HISTORICAL URL LOG VIEWING 1.00 K URLS OVER 1 DAY

Page 1 / 100 > >> Refresh

DETAILED URLS STORED SINCE: 11:10 09/22/12 (9 WEEKS 20 HOURS 36 MINUTES)

Search the Historical URL Log:

Client: All Clients — Ex. 10.0.0.0/8, group Intranet, user@DHCP (More)

URL Destination: All URL Destinations — Ex. example.com, example.com/image.gif (More)

Search

Url	Client	User	Groups	Bytes	Timestamp	Contents
safebrowsing-cache.google.com/safeb...	192.168.1.102	EVdesktop@tonann.com	Internal	309 B	Nov 25, 2012 06:40	Files
192.168.1.102:2869/upnphost/udhisap...	192.168.1.223	NAS@tonann.com	Internal	170 B	Nov 25, 2012 06:36	Other
safebrowsing-cache.google.com/safeb...	192.168.1.104	EVMacWL@tonann.com	Internal	309 B	Nov 25, 2012 06:39	Files
source.repository.backtrack-linux.o...	192.168.1.211		Internal	189 B	Nov 25, 2012 06:33	Other
all.repository.backtrack-linux.org/...	192.168.1.211		Internal	188 B	Nov 25, 2012 06:33	Other
64.repository.backtrack-linux.org/d...	192.168.1.211		Internal	189 B	Nov 25, 2012 06:33	Other
192.168.1.102:2869/upnphost/udhisap...	192.168.1.223	NAS@tonann.com	Internal	170 B	Nov 25, 2012 06:34	Other
weather.service.msn.com/data.aspx?s...	192.168.1.102	EVdesktop@tonann.com	Internal	321 B	Nov 25, 2012 06:25	Text
192.168.1.102:2869/upnphost/udhisap...	192.168.1.223	NAS@tonann.com	Internal	170 B	Nov 25, 2012 06:26	Other
192.168.1.102:2869/upnphost/udhisap...	192.168.1.223	NAS@tonann.com	Internal	170 B	Nov 25, 2012 06:29	Other

For assistance with this product, please contact support@arbornetworks.com.

ARBOR NETWORKS

5. 優れたレポート機能

“豊富なレポート・オプションにより
用途に合わせたグラフィカルなレポートを作成できます”

- Traffic
  - Top Hosts
  - Top Services
  - Top Users
- Entity
  - Entity Information
  - Single Entity to Entity
  - Multiple Entity to Entity
- Web
  - Web Usage Summary
  - URL Log
- Network
  - Interface
  - Router
  - Interface Object
- Policy
  - Rules and Events
  - Alert Summary
  - Alert Details
- System
  - Audit Trail
  - System Summary
- Custom Reports
  - create New Custom Report

“レポートの最大保管数は 3,650 となり1日毎に
レポートを作成した場合、約10年分が保管されます”

ARBOR NETWORKS

5. 優れたレポート機能

“レポートはPDF・CSV・XLSにより出力可能です”

REPORT 4 : TOP SERVICES REPORT

29 Oct 2012 18:16 to 30 Oct 2012 18:16 (1 Day)

Save or Schedule

User Comments

example report

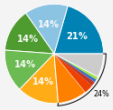
Report Description

The Top Services Report aggregates all traffic seen over a given period of time presents the top n-many services and applications ranked by total bytes. This report can tell one which services and applications are responsible for the largest traffic volume on the network.

During the period 18:16 29/10/12 to 18:16 30/10/12 (1 day 0h00m), these were the top 10 services ranked according to how many bytes were associated with each. In this report, the top service was UDP/63.

TOP 10 SERVICES

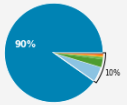
Key	Service	Applications	Bytes	bps	Percent	Service Groups
	UDP/63		330.98 G	30.65 Mbps	21%	
	UDP/5000	< 1% NTP	229.35 G	21.24 Mbps	14%	
	UDP/111 (RPC)		226.76 G	21.00 Mbps	14%	RPC
	UDP/69 (TFTP)	< 1% TFTP	223.67 G	20.71 Mbps	14%	TFTP
	UDP/135		219.27 G	20.30 Mbps	14%	
	TCP/80 (HTTP)	53% HTTP, < 1% NTP, < 1% LPD, < 1% NetFlow, < 1% AFS	155.03 G	14.36 Mbps	10%	HTTP
	TCP/443 (HTTPS)	17% SSL, < 1% NTP, < 1% LPD, < 1% LDAP, < 1% HTTP	47.44 G	4.39 Mbps	3%	HTTPS
	ICMP/8/0 (echo_request)		22.92 G	2.12 Mbps	1%	echo_request
	TCP/25 (SMTP)	19% SMTP, < 1% SSL, < 1% LPD, < 1% NTP, < 1% HTTP	16.71 G	1.55 Mbps	1%	SMTP
	UDP/31373		15.86 G	1.47 Mbps	1%	
	Other (124.97 k services)		123.85 G	11.47 Mbps	7.7%	



During the period 18:16 29/10/12 to 18:16 30/10/12 (1 day 0h00m), these were the top 10 applications ranked according to how much traffic was seen for each application. In this report, the top application was None.

TOP 10 APPLICATIONS

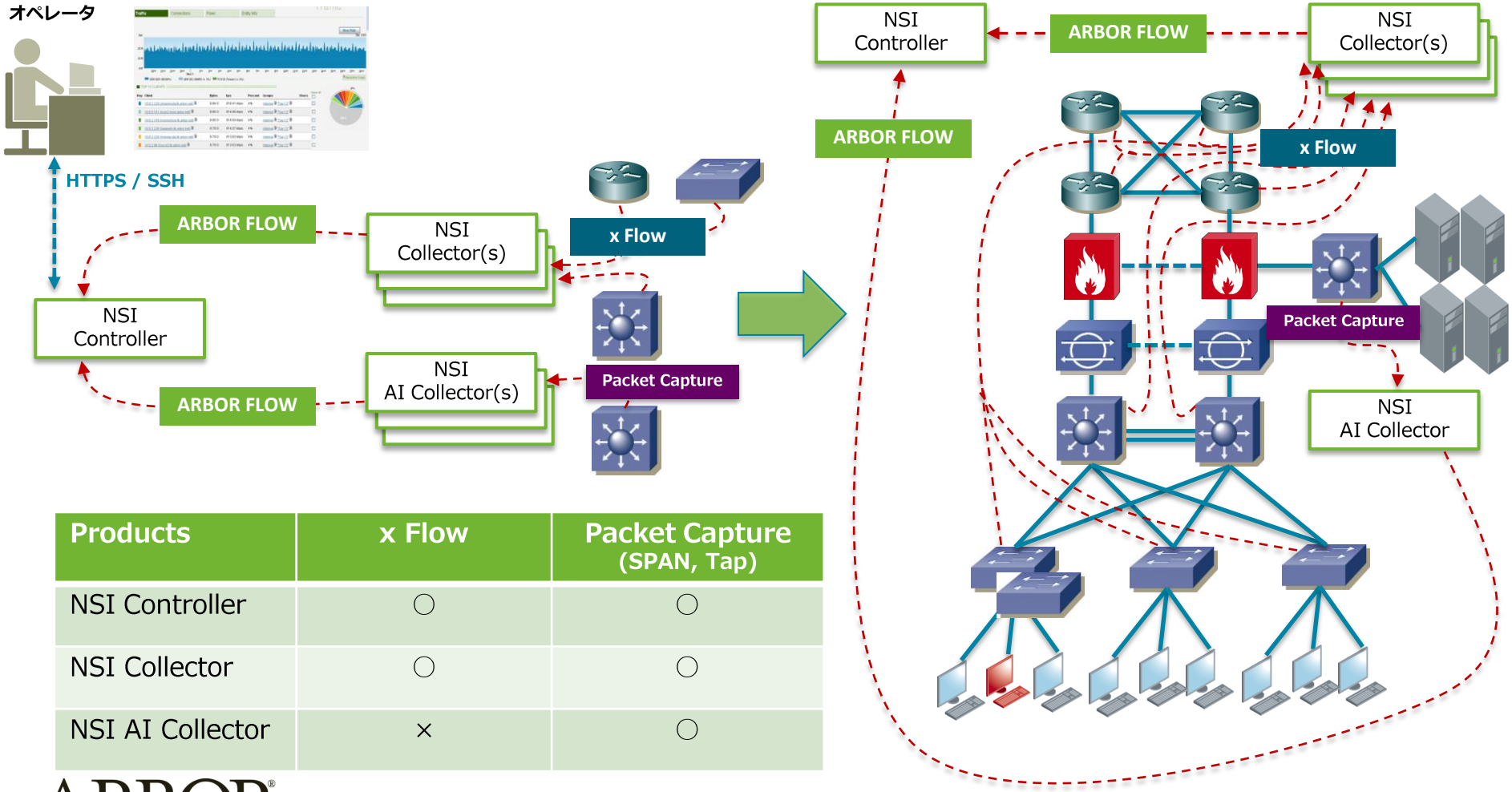
Key	App Name	Bytes	bps	Percent
	Unknown	2.15 T	198.94 Mbps	90%
	HTTP	120.47 G	11.15 Mbps	5%
	SSL	60.81 G	5.63 Mbps	2%
	NTP	18.69 G	1.73 Mbps	0%
	RDP	8.80 G	815.23 kbps	0%
	ICY	8.37 G	775.32 kbps	0%
	SMTP	5.03 G	466.10 kbps	0%
	BitTorrent	4.26 G	394.27 kbps	0%
	DNS	3.29 G	304.67 kbps	0%
	SSH	1.53 G	141.67 kbps	0%



ARBOR NETWORKS

Pravail NSI モニタリング構成

“最小構成は、コントローラ x 1台となります”



Products	x Flow	Packet Capture (SPAN, Tap)
NSI Controller	○	○
NSI Collector	○	○
NSI AI Collector	×	○

Pravail NSI

セキュリティ・インテリジェンス
- マルウェアなど悪意のあるソフトウェアを監視する。

グローバル & エンタープライズ視認性
- 視認性を提供しリスク・プロファイルによるアラートを作成。

コントローラ

アップグレード　アップグレード　アップグレード

Controller	5110	5120	5130	5220	5230
フロー / 秒 (直接)	3,500 FPS	10,000 FPS	35,000 FPS	25,000 FPS	80,000 FPS
最大フロー / 秒 (直接 + コレクター)	100,000 FPS	100,000 FPS	100,000 FPS	250,000 FPS	250,000 FPS
発信元数	10	250	500	500	500
最大コレクター数	3	30	30	50	50
DHM	×	×	×	○	○
フロー・ストレージ	300GB	300GB	300GB	1.2TB	1.2TB
インターフェイス	• 4 x 10/100/1000 Copper • 4 x 1G (GE or SX or LX) • 2 x 10G Fiber (SR or LR) • 2 x 10/100/1000 Copper *管理ポート				

- それぞれのプラットフォームにおいて、上位機種へソフトウェアライセンスによるアップグレードが可能です。
- コントローラは最低1台必要となります。
- 追跡可能なID数(100,000)。ADとの連携も可能です。

ARBOR NETWORKS

Pravail NSI

コレクター

アップグレード　アップグレード　アップグレード

Collector	5003 AI	5004	5005	5006	5007
フロー / 秒	該当なし	8,000 FPS	16,000 FPS	35,000 FPS	80,000 FPS
スループット	1 Gbps	該当なし	該当なし	該当なし	該当なし
インターフェイス	• 4 x 10/100/1000 Copper • 4 x 1G (GE or SX or LX) • 2 x 10G Fiber (SR or LR) • 2 x 10/100/1000 Copper *管理ポート				

- それぞれのプラットフォームにおいて、上位機種へソフトウェアライセンスによるアップグレードが可能です。
- コレクターはコントローラと組み合わせて使用します。単体では動作いたしません。
- AI (Application Intelligence) コントローラはパケット・データのみを解析します。

ARBOR NETWORKS

x Flowの種類

- ネットワーク・ベンダーによって開発された多くのIP Flowが存在します。
  - **IPFIX** IETF (standard)
  - **cFlow** Alcatel-Lucent
  - **Netflow** Cisco
  - **rFlow** Ericsson
  - **Netstream** HP/3Com, Huawei Tech.
  - **cFlow, jFlow** Juniper
  - **sFlow:**

    Alaxala, Alcatel-Lucent, Allied Telesis, Arista Networks, Brocade, Cisco, Comtec Systems, Dax Networks, Dell, D-Link, Enterasys, Extreme Networks, Fortinet, HP, Hitachi, Huawei, IBM, Juniper Networks, NEC, Netgear, Vyatta, ZTE, ZyXEL

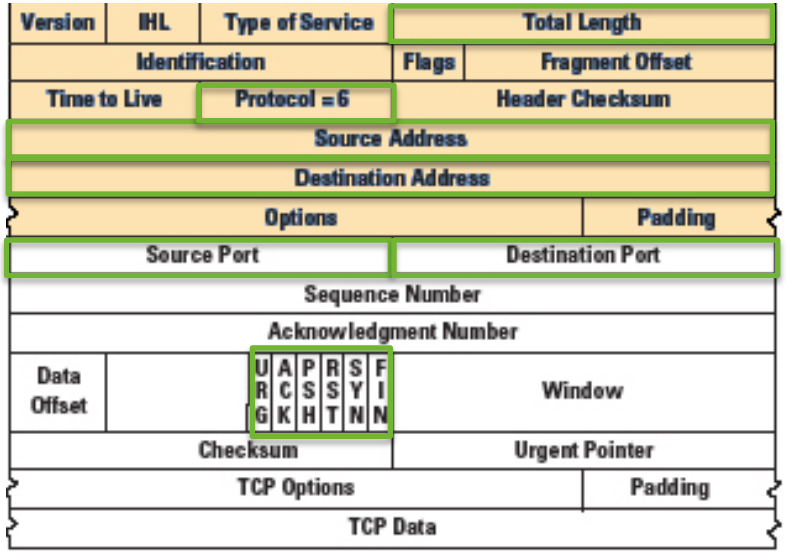
ARBOR NETWORKS

NetFlowの情報

- NetFlow によって、トラフィック・フロー を「見える化」し
  ネットワークのベースライン、トレンドを取得することができます。

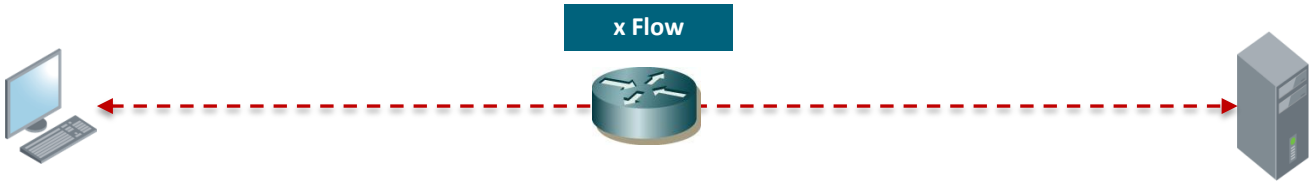
The 5 tuple

- Source IP Address
- Destination IP Address
- Source Port
- Destination Port
- Layer3 Protocol



Network metrics

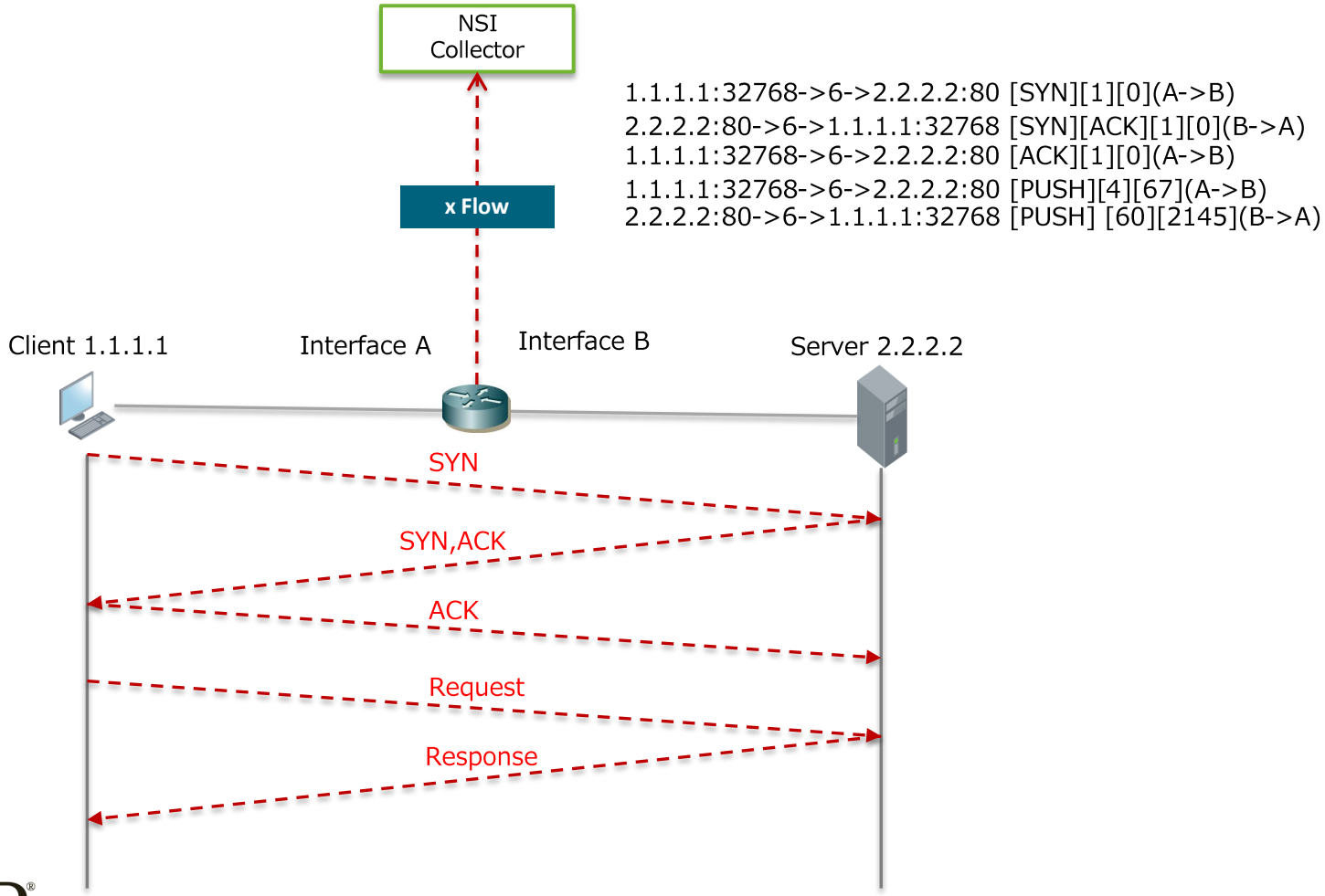
- Packet count
- Byte count
- TCP Flags
- Ingress ifindex
- Egress ifindex



ARBOR NETWORKS

NetFlowの仕組み

- Router・SwitchのNetFlowにより、視認性を提供します。



Cisco Netflow Support

Device	OS	Netflow	Notes
Cisco Carrier Routing System (CRS)	IOS XR	FNF	・CSCtq11911 : Setting destination port in exporter map on TAIKO is not working Fixed 4.2(0.6)I, 4.1(1,24)I, 4.0(4.6)I
ASR 9000 Series Aggregation Service Routers	IOS XR	FNF	・CSCtr62137 : netflow exporter is disabled with BGP recursive route to exporter Fixed 4.2(0.12)I,4.0(4.14)I, 4.1(2.12)I
ASR 1000 Series Aggregation Service Routers	IOS XE	TNF and FNF	・Netflow top talkers feature is not supported yet on ASR1K
Cisco XR 12000/12000 Series Router (GSR)	IOS	FNF	・CSCtd62350 : GSR netflow vrf-aware dropping packets Fixed 12.0(32.9.23)SY, 12.0(32)SY11, 12.0(33.5.39)S, etc
Cisco 7600 Series Router	IOS	TNF	・CSCsm59802 :"ip flow egress" has no affect on a 7600 series router Fixed 12.2(32.8.22)REC186, 12.2(33)ZI
Cisco ISR G2 (3900, 2900, 1900, 800 Series)	IOS	TNF and FNF	・CSCto53635 : netflow always use default cache entry size after reboot Fixed 15.0(1)M5.5, 15.2(0.12)T, etc
Cisco ISR G1 (3800, 2800, 1800 Series)	IOS	TNF and FNF	none
Nexus 7000 * Not support Nexus 5000	NX-OS	FNF	・F2-Series module or M1,2-Series module (not support F1-Series module) ・CSCso91787 : Incorrect TCP Flags shown in netflow table Fixed 4.0(1.42)
Nexus 1000V	NX-OS	FNF	・CSCtn69289 : netflow error on port-profile with port-channel cryptic Fixed 4.2(1)SC1(4a)
Catalyst 6500 with SUP2T	IOS	FNF	・Supervisor Engine 2T with Policy Feature Card 4 (PFC4) ・15.0(1)SY later (does not work in 12.2(50)SY)
Catalyst 6500 with SUP32, SUP720	IOS	TNF	・CSCsa79630 : Cat6500 Netflow does not export all flows Fixed 12.2(18)SXF2, 12,2(18.9.20)SX3.21, etc ・CSCsh99774 : Netflow Data Export on VRF specific export destination address Fixed 12.2(32.8.11)XR45.11, 12.2(33)SXI
Catalyst 4500 and 4500X with SUP7	IOS	FNF	・4500 + Supervisor Engine V-10GE ・4500 + Supervisor Engine Ⅳ or V + Netflow Service Card (WS-F4531)
Catalyst C3KX-SM-10G	IOS	FNF	・Network Services Module (C3KX-SM-10G) ・15.0(1)SE and IP Base or IP Services (not support LAN Base)

TNF: Traditional Netflow FNF: Flexible Netflow

※2013年1月の情報です。

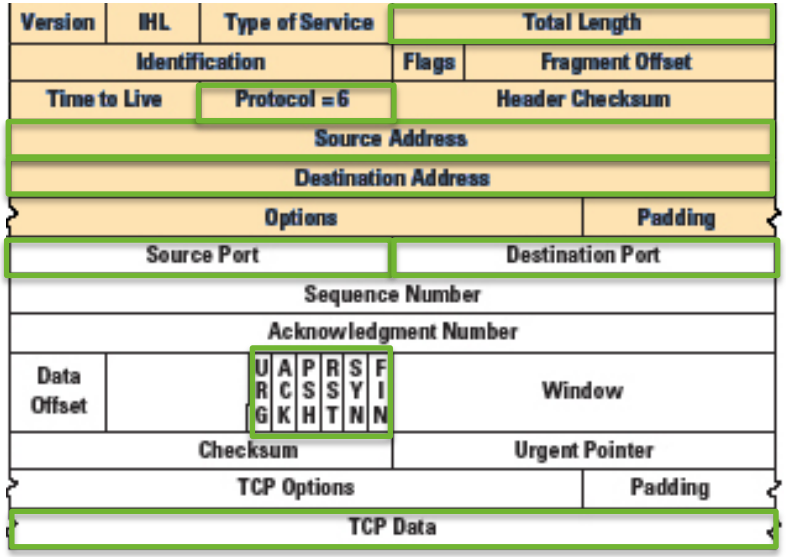
Packet Captureの情報

- AI Collectorは、パケット・キャプチャによりTCPペイロードを検査し、アプリケーションを識別します。

The 5 tuple

- Source IP Address
- Destination IP Address
- Source Port
- Destination Port
- Layer3 Protocol

[TCP Header + TCP Payload]

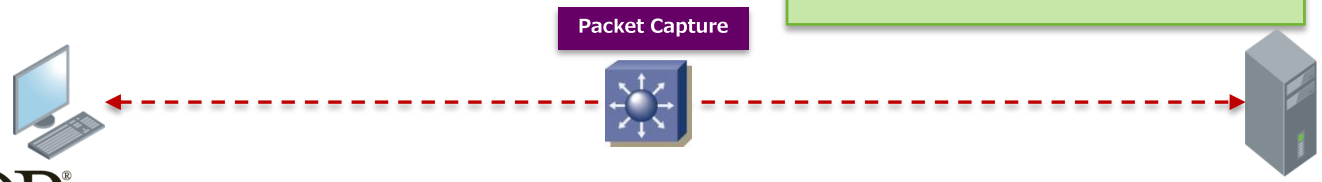


Network metrics

- Packet count
- Byte count
- TCP Flags
- Ingress ifindex
- Egress ifindex

Payload inspection

- Application Identification



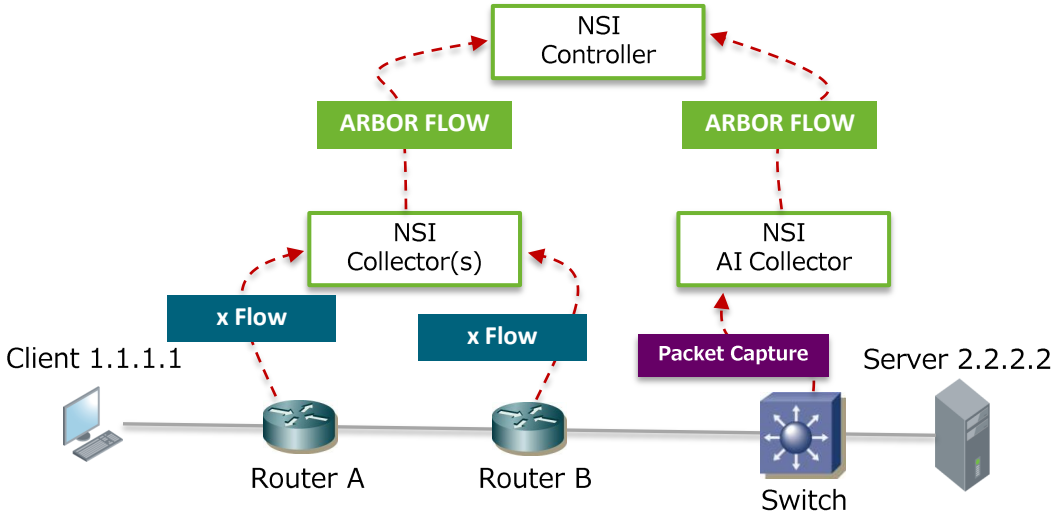
Stateful Flow Reassembly

- コントローラ は、ネットワーク上の複数のコレクタから生成された トラフィック・データを集約することで、信頼性を保ちます。

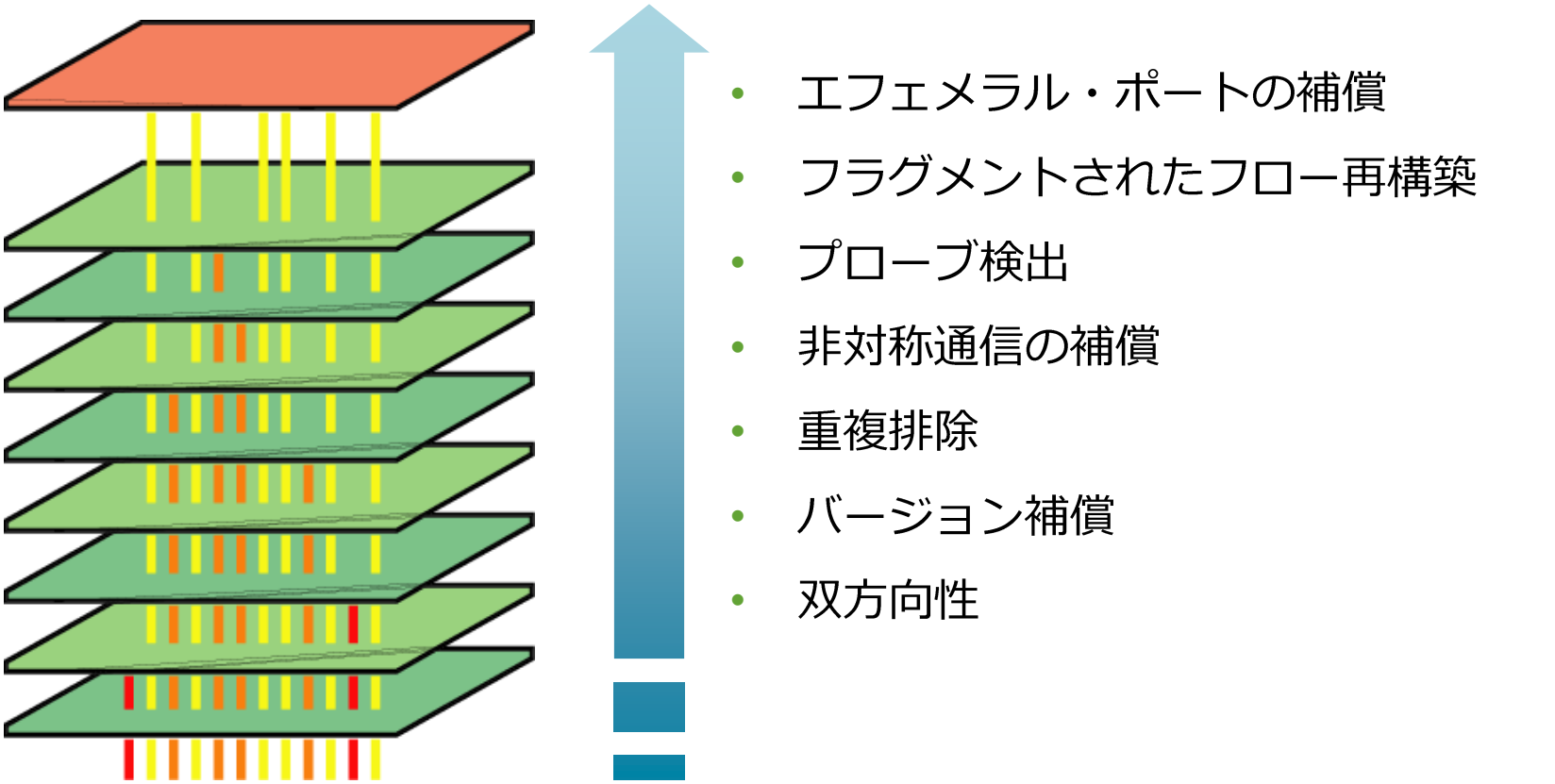
<NSI Controller トラフィック・データ>

Collector A: 1.1.1.1:32768->6->2.2.2.2:80 [SYN][1][0](A->B)
~~**Collector B:** 1.1.1.1:32768->6->2.2.2.2:80 [SYN][1][0](A->B)~~
Collector A: 2.2.2.2:80->6->1.1.1.1:32768 [SYN][ACK][1][0](B->A)
~~**AI Collector:** 1.1.1.1:32768->6->2.2.2.2:80 [SYN][1][0](A->B)~~
~~**Collector B:** 2.2.2.2:80->6->1.1.1.1:32768 [SYN][ACK][1][0](B->A)~~
AI Collector: 1.1.1.1:32768->6->2.2.2.2:80 [ACK][1][0](A->B)
~~**AI Collector:** 2.2.2.2:80->6->1.1.1.1:32768 [SYN][ACK][1][0](B->A)~~

重複排除



Stateful Flow Reassembly (Cont.)

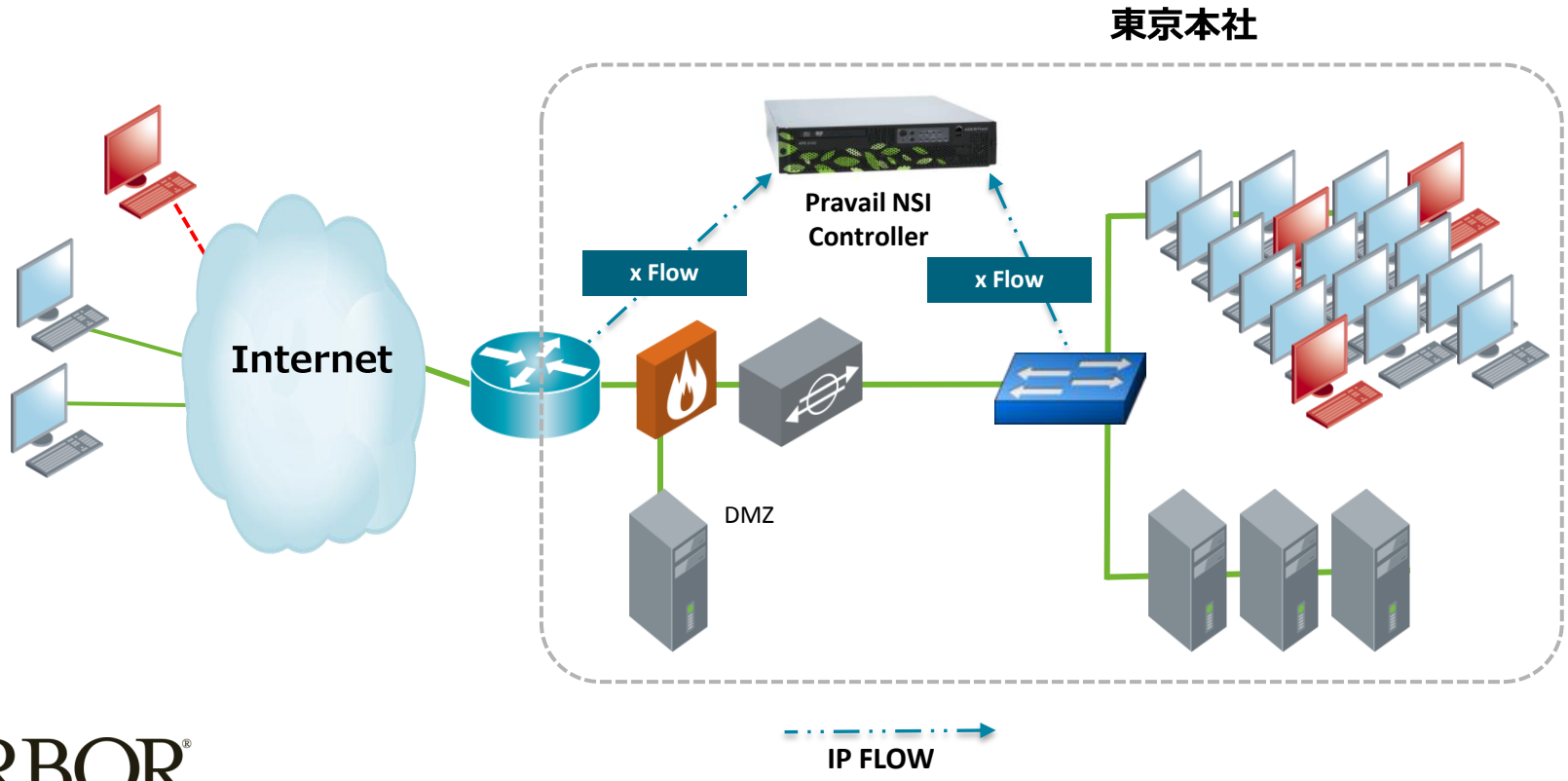


- エフェメラル・ポートの補償
- フラグメントされたフロー再構築
- プローブ検出
- 非対称通信の補償
- 重複排除
- バージョン補償
- 双方向性

ARBOR NETWORKS

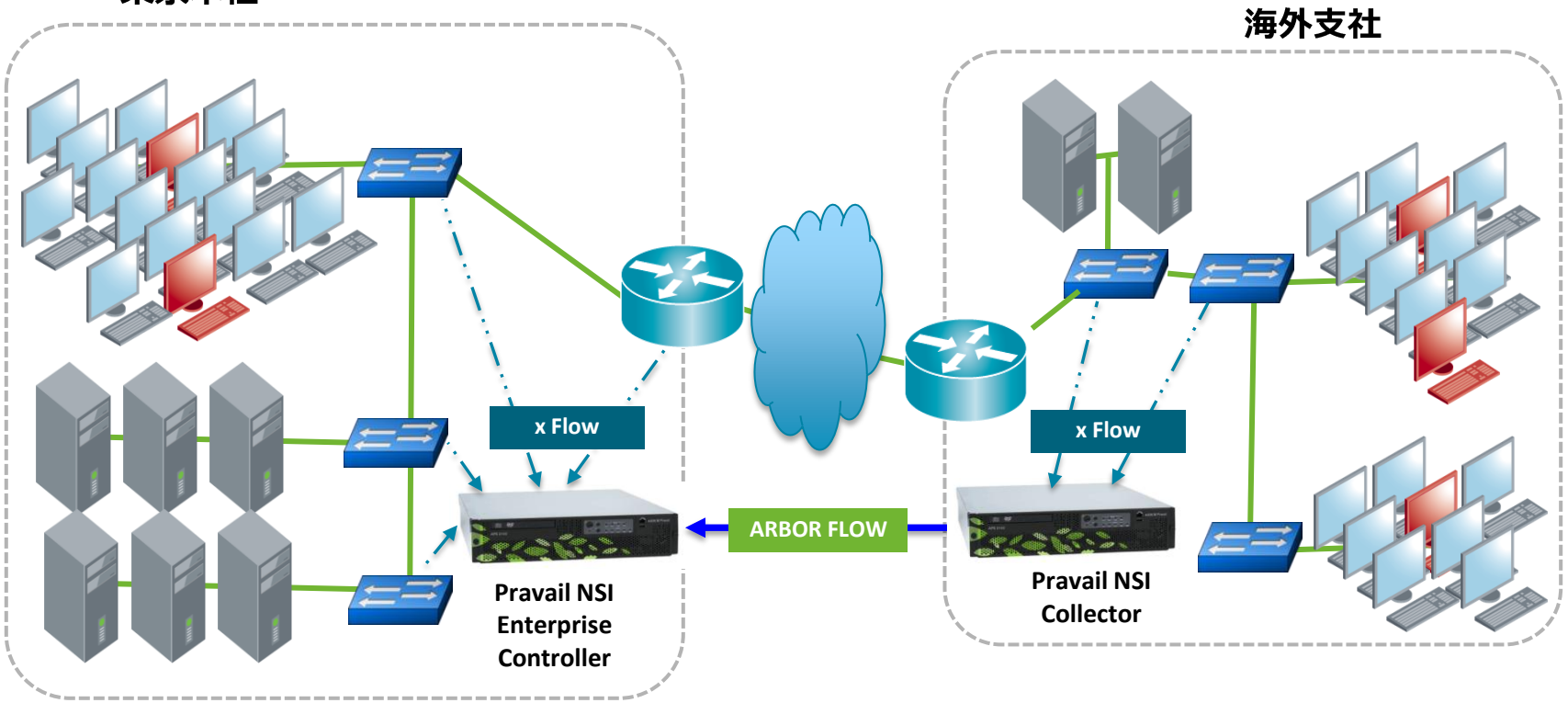
Pravail NSI 導入シナリオ (1)

- **本社**
  - RouterおよびSwitchからのxFlowを使用しコントローラによって、ネットワークの視認性を提供します。（SPANによるパケット・キャプチャも可能です）



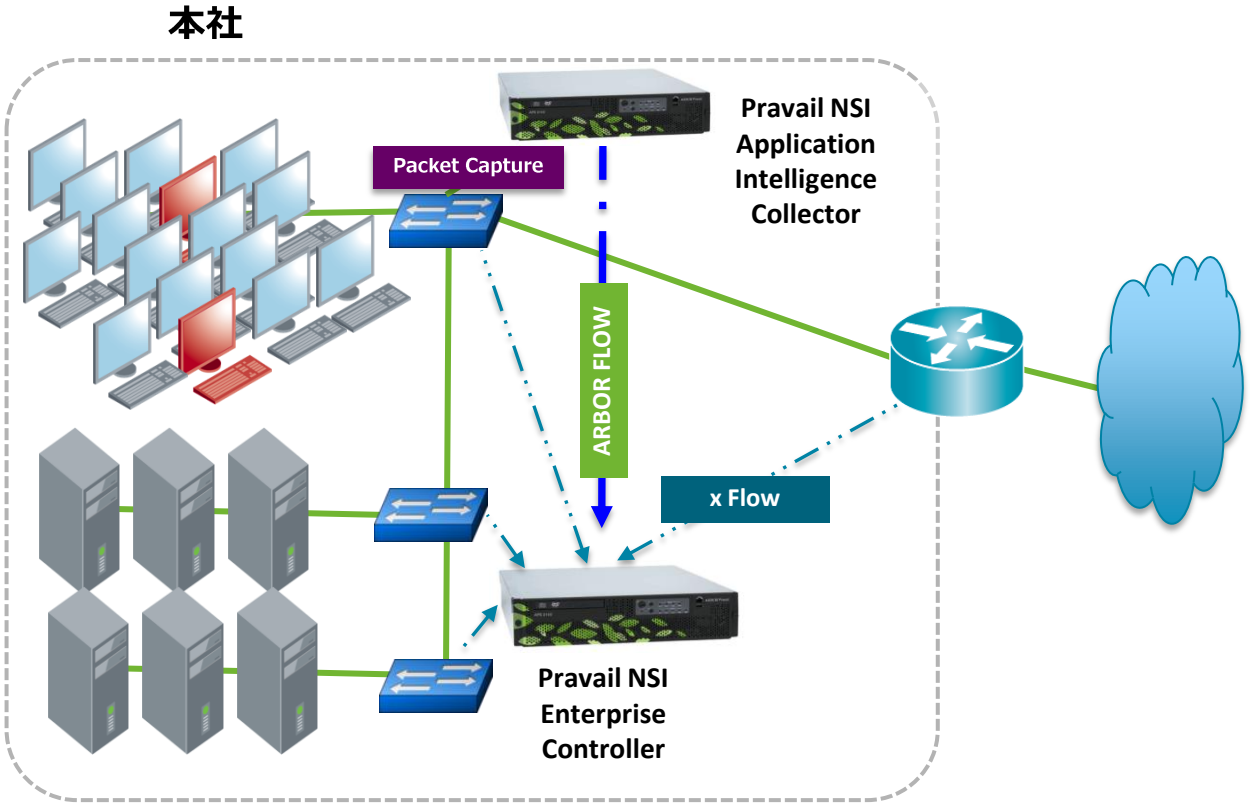
Pravail NSI 導入シナリオ (2)

- **複数拠点 (本社 + 支社)**
  - 支社側にコレクターを導入しxFlowを収集。
    収集した情報を本社のコントローラに送ることで
    広範囲の視認性を提供します。



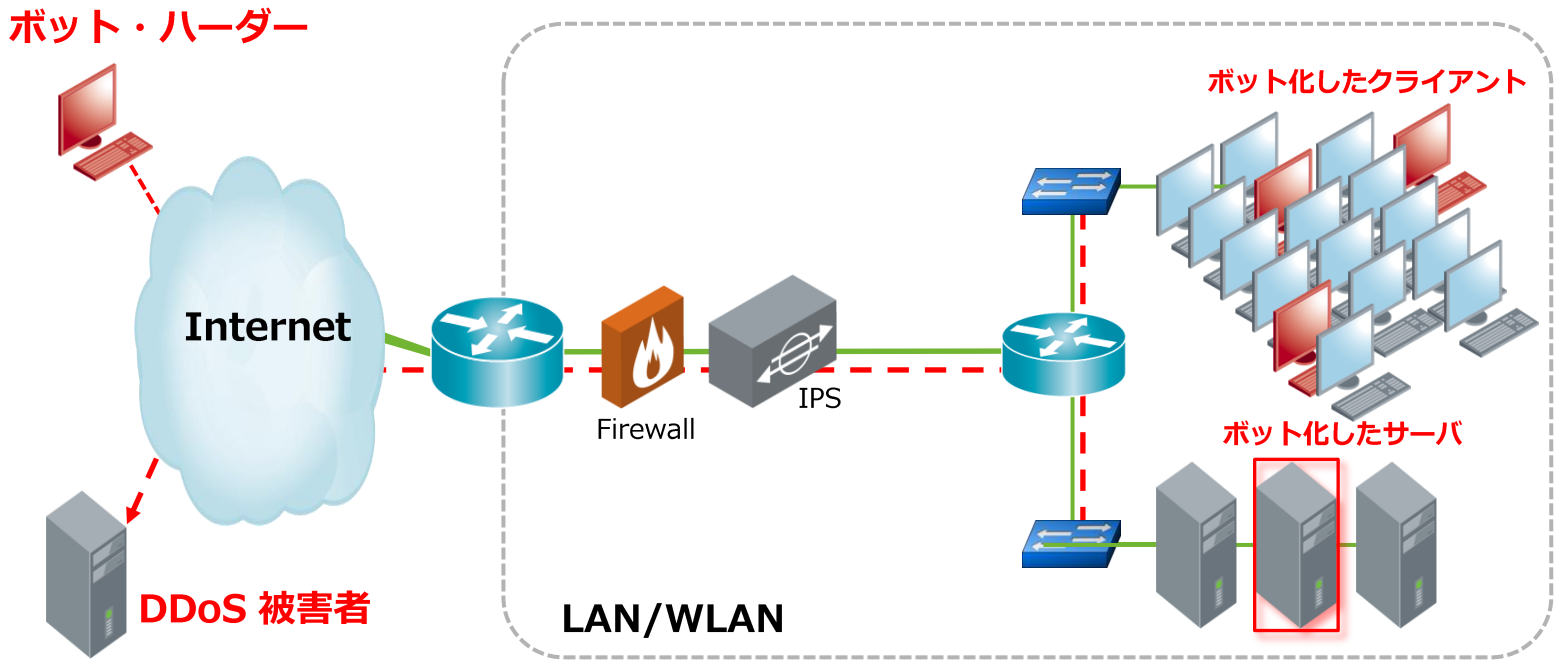
Pravail NSI 導入シナリオ (3)

- **本社拡張 (コントローラ + AIコレクター)**
  - AI (アプリケーション・インテリジェンス)を導入し
    パケット・データを収集。コントローラに情報を送ることで
    P2Pやインスタント・メッセージなど、アプリケーションの
    不正使用を検知し、情報漏洩を未然に防ぎます。



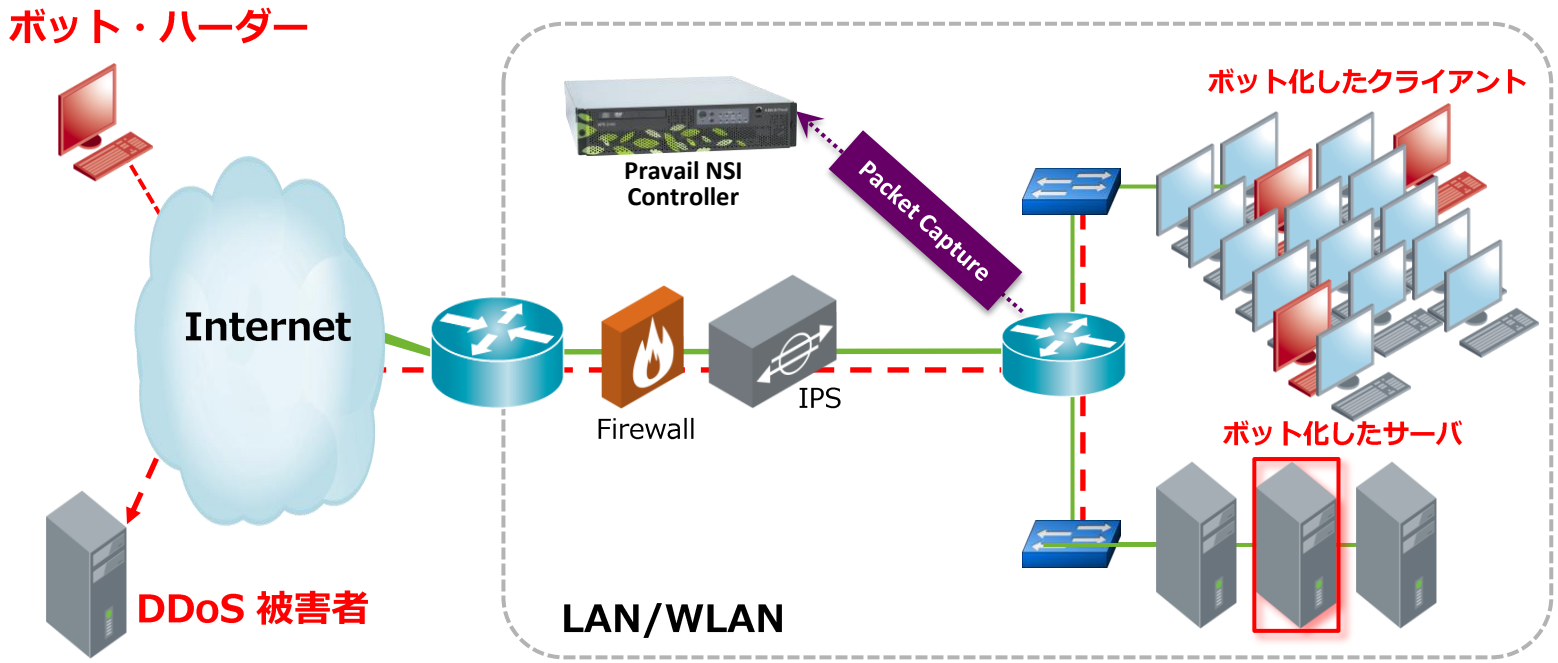
ケース1 (ボット化したホストのDDoS攻撃加担)

- ISPからの調査報告により、自社のネットワークからDDoS攻撃をしていることが確認され、これを停止するよう要求がありました。
  - ネットワーク内のホストがボットの一部となり、WAN回線の帯域幅はDDoS被害者への攻撃で使い果たしています。



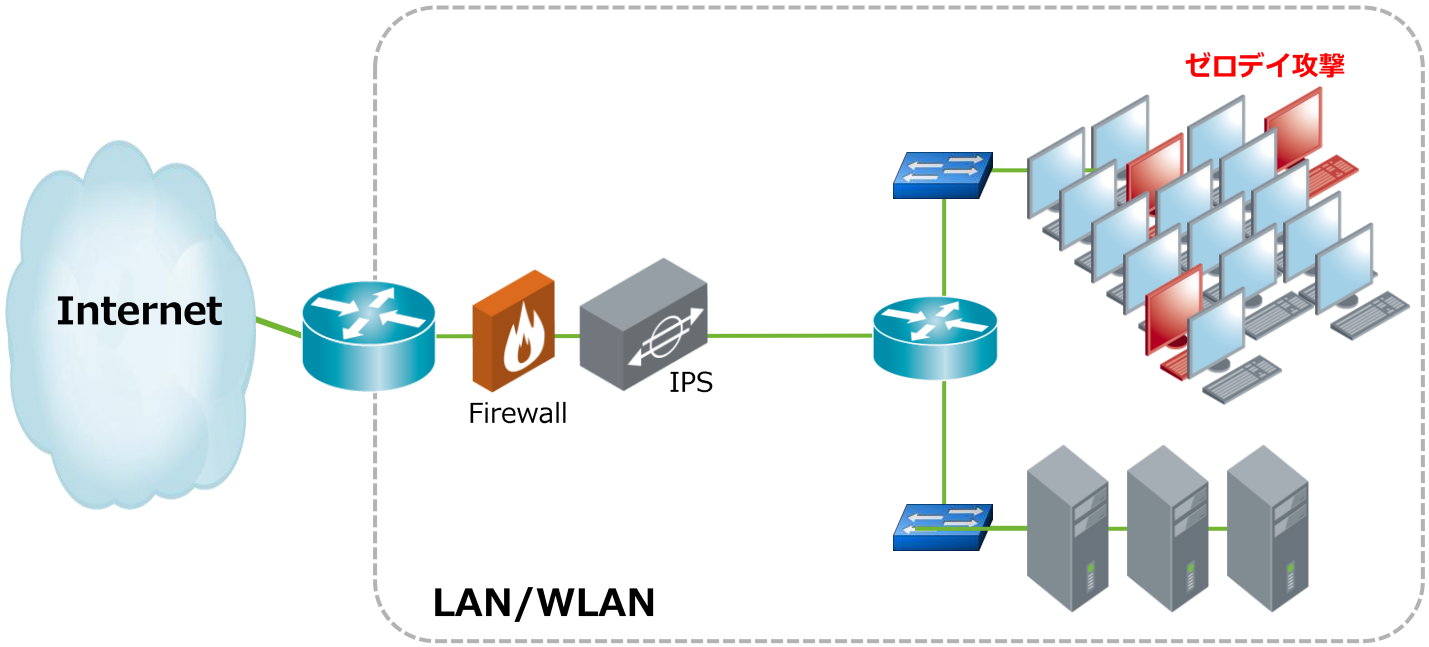
解決策1（ボットの検出・駆除）

- Pravail NSIを導入し、キャプチャーされたトラフィックを分析することにより、ネットワーク内のボットを見つけ出しました。
  - Pravail NSI は、ATFと呼ばれる”フィンガープリント”を使用してボット化したホストを検知します。



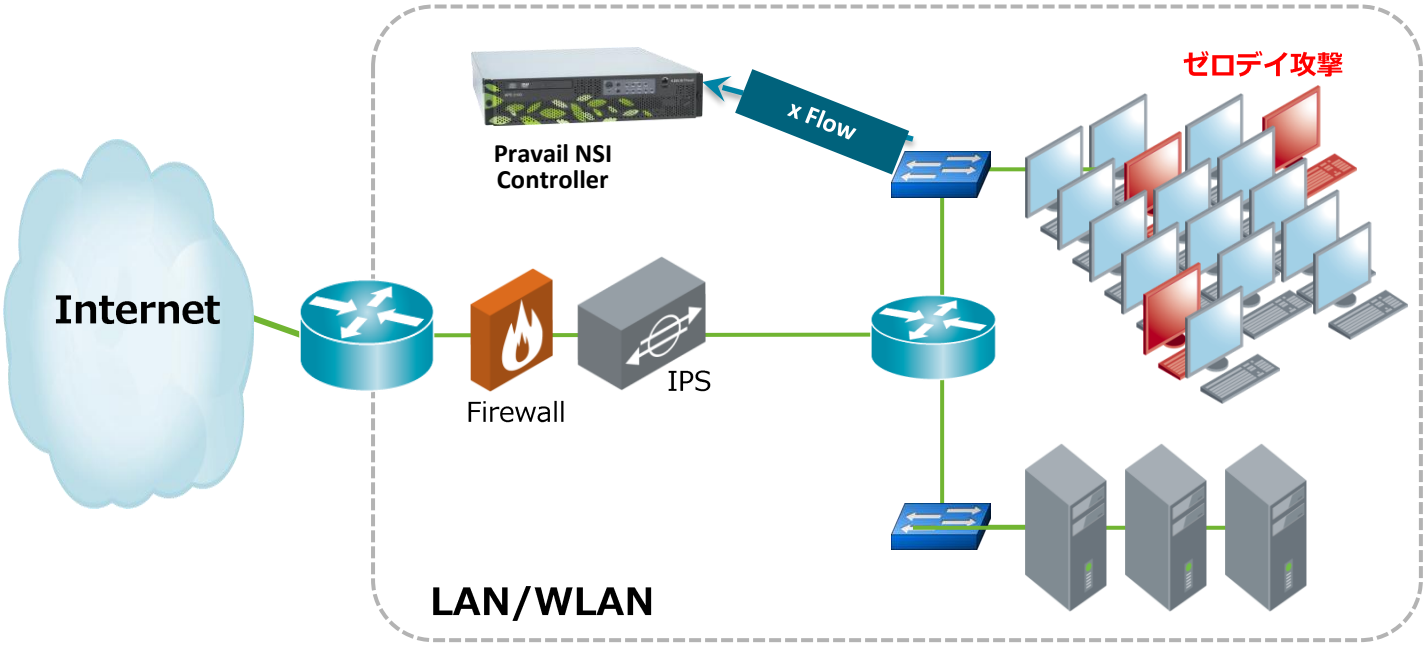
ケース2（ゼロデイ攻撃）

- アンチウィルスやIDSシグネチャーを更新したにも関わらず
  明らかにいくつかのワークステーションは未知のマルウェアに
  感染してしまいました。（典型的なゼロデイ攻撃）
  - 顧客は、マルウェアに感染したホストを見つけ出して駆除したい。



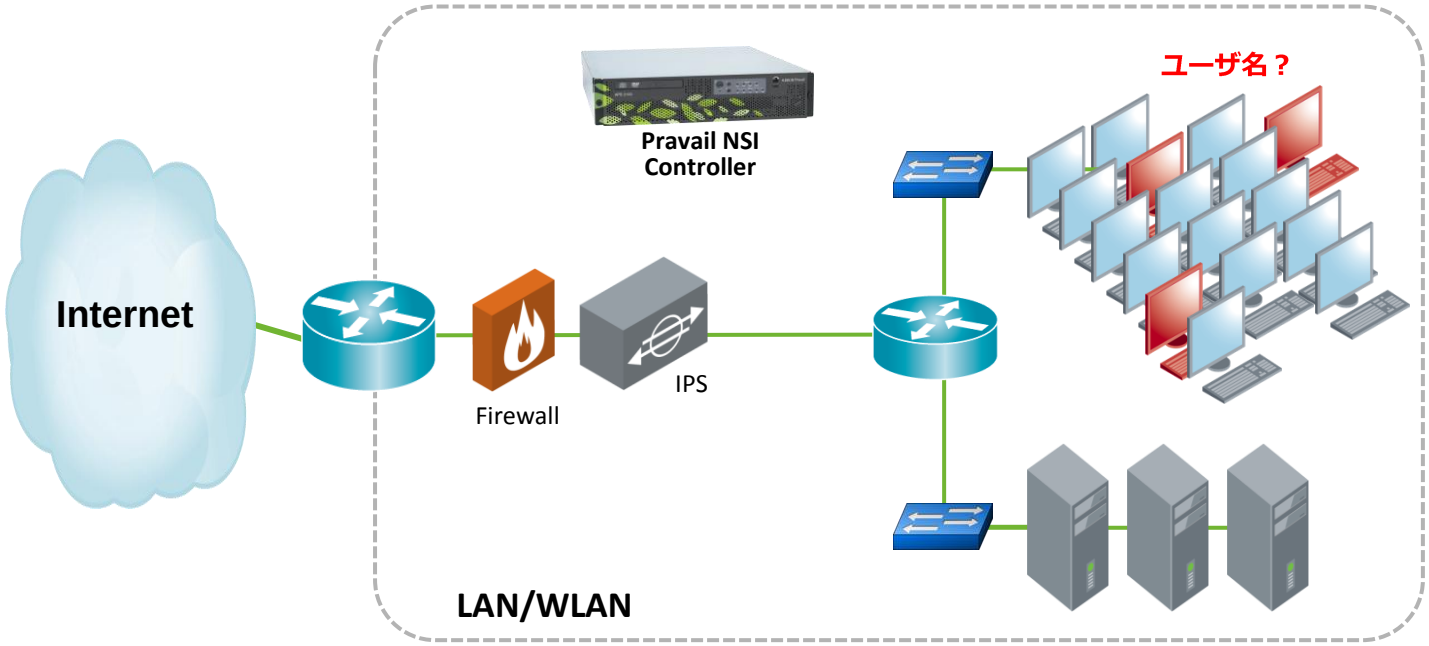
解決策2（マルウェアの検出・駆除）

- Pravail NSI を導入し、内部ネットワークを監視することによって
  マルウェアの活動を検出します。
  - 平均3Gbpsをパケットキャプチャする代わりにスイッチから
    xFlow情報を受信することで効率的に検出します。
    (パケットキャプチャに比べxFlowのトラフィック量は約1%です)



ケース3（ユーザ名は？）

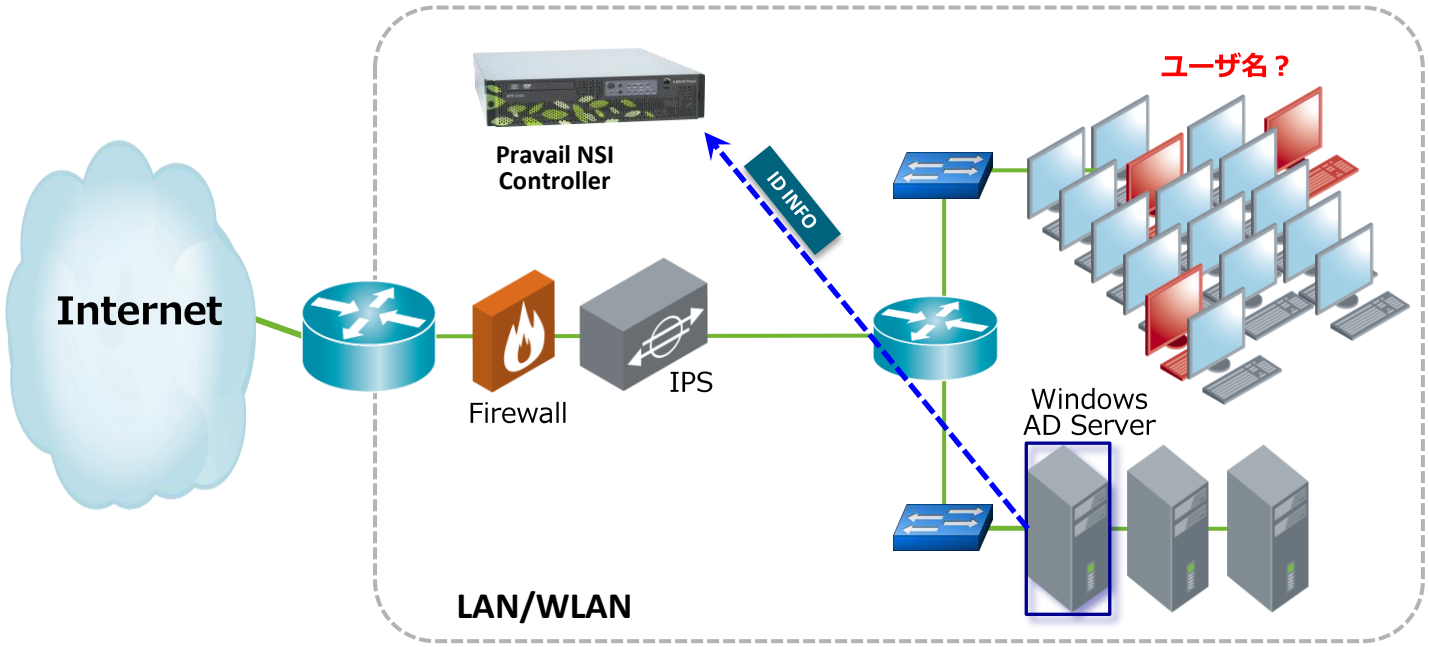
- Pravail NSIを既に導入し顧客は、ネットワーク上の脅威の検出および可視性に非常に満足しておりますが、ユーザ名を使用したレポートを表示したいと要望がありました。
  - この要望は、IPアドレスが時間の経過と共に変化することを考慮すると非常に役立つ情報となります。



解決策3（ADと連携し、ユーザ情報を付加）

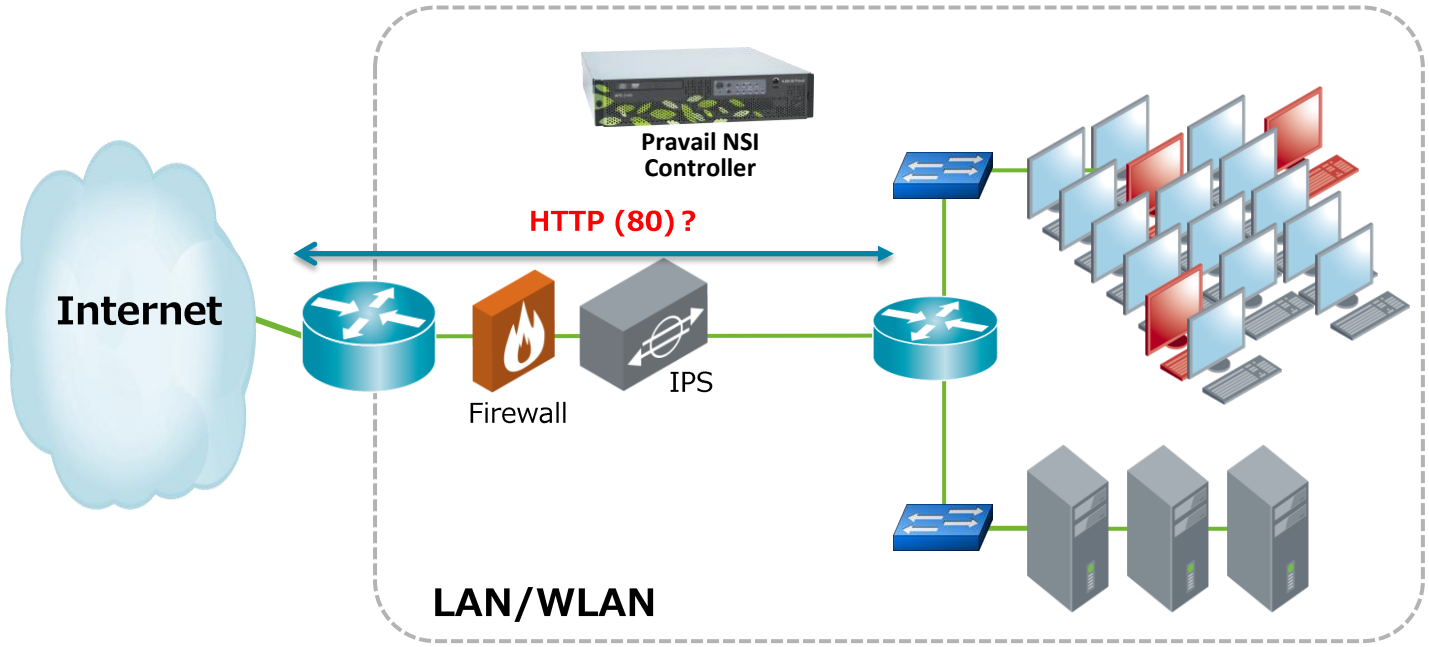
- Pravail NSIとActive Directoryが連携することにより、レポートにユーザ情報を付加できます。

“AuthXサービスにより、ユーザ情報は暗号化されて転送されます”



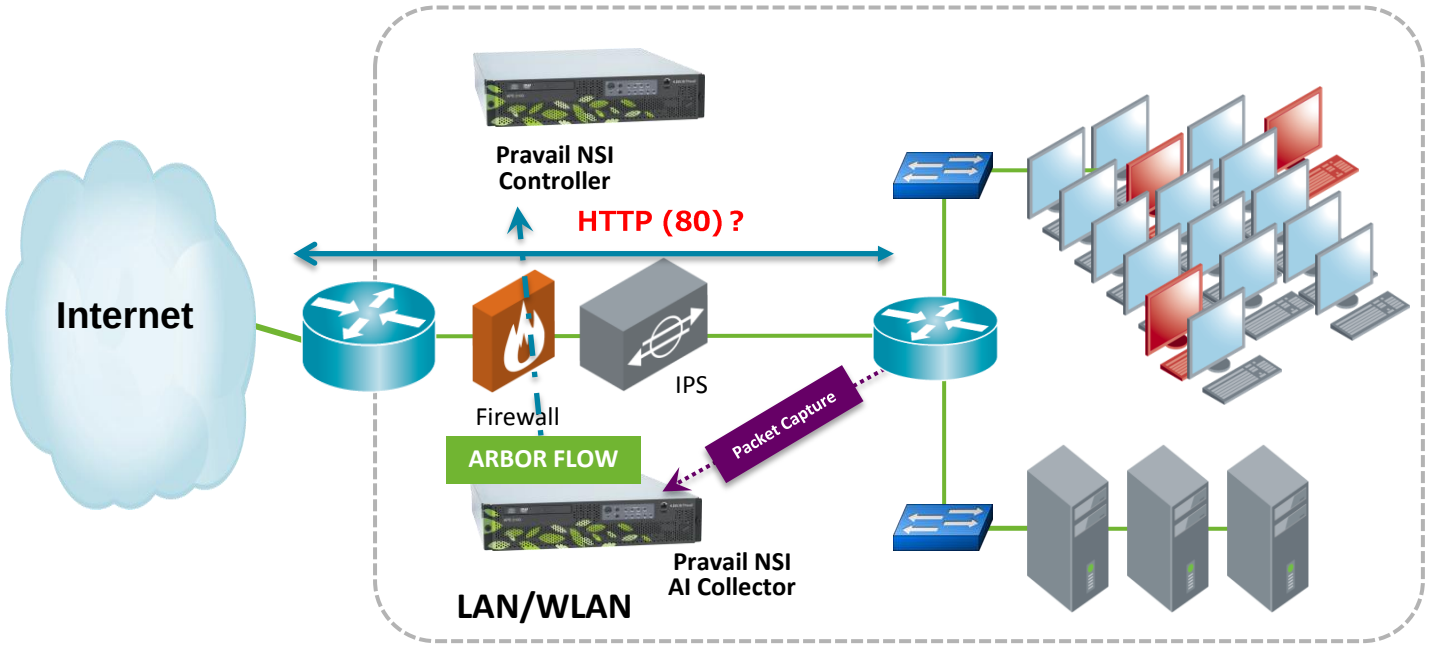
ケース4（過剰なHTTPトラフィック？）

- トラフィック統計を確認すると、内部と外部の両方でポート80を使用したHTTPトラフィックが、かなりのボリュームを占めています。セキュリティ・チームは、80番ポートに隠されたP2P、インスタント・メッセージなどの不正使用を確認する必要があります。



解決策4（AIコレクターの導入）

- ネットワークの主要L3スイッチのSPANによって受け取った
  キャプチャ・データをAIコレクターで分析し、既に導入済みの
  コントローラに情報を転送することにより、総合的な
  視認性を提供します。



ターゲットとなる市場

銀行

ホスティング・
プロバイダ

オンライン・
ショッピング

医療

政府

教育

商談シナリオ: 銀行

ビジネス

- 国内店舗・海外営業所などいくつかの
  オフィスを持つ大規模な銀行。
- 従業員はWindowsデスクトップを使用しており
  インターネットのアクセスを許可されてています。
- PCにアンチウィルス・ソフトウェアを導入
  しているにも関わらず、マルウェアに関する
  問題を抱えています。
- ネットワーク管理はアウトソーシングされています。

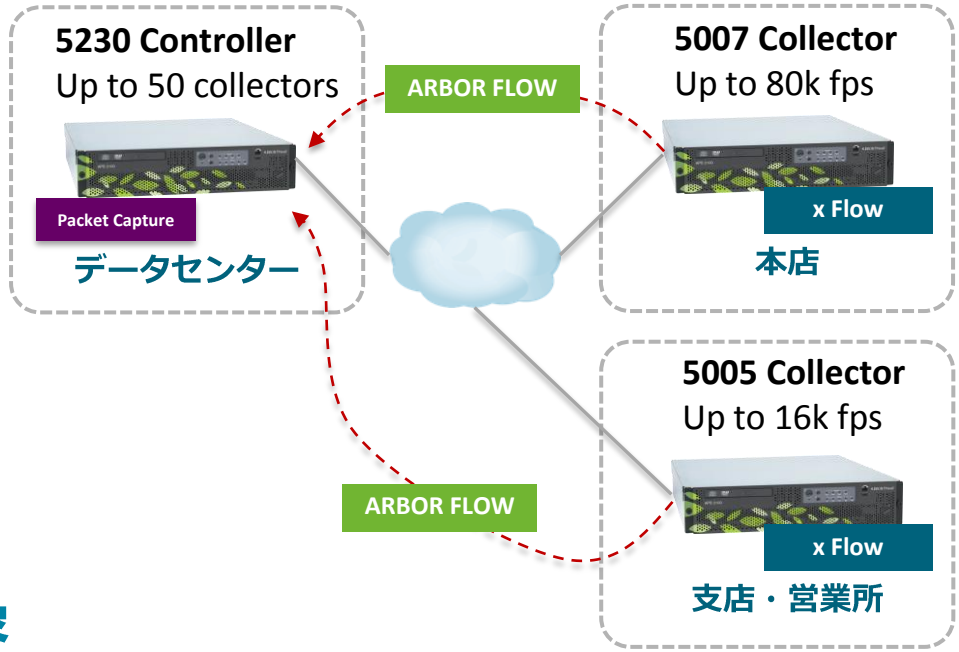
プロジェクト

- ネットワークに存在するリスクを識別し、必要に応じて効果的な
  セキュリティ・インテリジェンス・ソリューションを探しています。
- 解決策は、国内店舗・海外営業所などいくつかのオフィスに存在する
  複数LANセグメントのトラフィックを本店で一元管理することです。

商談シナリオ: 銀行

ネットワーク

- 本店(1)・支店(4)と営業所(30) で構成され、すべてイントラネットに接続されています。
- ITデータセンターが 存在します。



お見積り内容

1x 5230 + 34x 5005 + 1x 5007,
メンテナンス＆サポート、ATF（年次）

プロジェクト管理、設計・構築 + トレーニング

Total ~ 機器 + サービス + /年次サポート *

* 機器およびサポート費用の価格は販売代理店にお問い合わせください。

ARBOR NETWORKS

商談シナリオ: ホスティング・プロバイダ

ビジネス

- 1つの大規模な施設で何百もの顧客にインターネットを利用したホスティング・サービスを提供しています。
- ハッキングされた顧客のサーバは、DDoS攻撃を生成し、サービスと他のお客様へ被害をもたらします。

プロジェクト

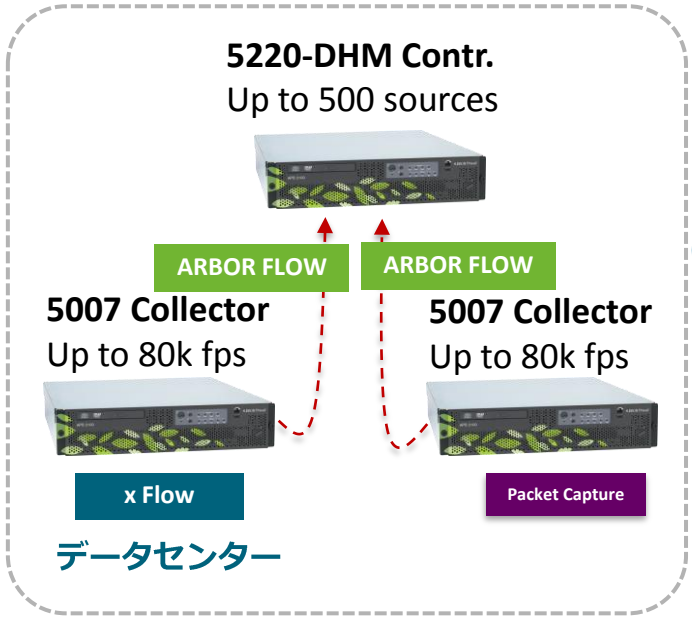
- 内部のトラフィックを分析したフォレンジックスを可能にするスケーラブルな方法を探しています。
- 大量のネットワーク・トラフィックを検査するソリューションが必要となります。

ARBOR NETWORKS

商談シナリオ: ホスティング・プロバイダ

ネットワーク

- インターネット接続に20Gbpsのリンクを持つ、1つのデータセンター。
- 200のホスティング・サービスを提供しています。



お見積り内容

1 5220-DHM + 2x 5007,
メンテナンス＆サポート、ATF（年次）

プロジェクト管理、設計・構築 + トレーニング

Total ~ 機器 + サービス + /年次サポート *

* 機器およびサポート費用の価格は販売代理店にお問い合わせください。

ARBOR NETWORKS

商談シナリオ: リモート・セールス (BYOD)

ビジネス

- BYODを含む様々なデバイスを活用し、ネットワーク・アプリケーションへ接続することにより、優れた販売力をもっています。
  - 2,000人のアカウント・マネージャの営業力は世界中で存在感を示しています。
  - ERPを使用して販売管理を行っています。
  - 販売サポートの情報は、e-mailまたはイントラネットのWebにアクセスして得ています。

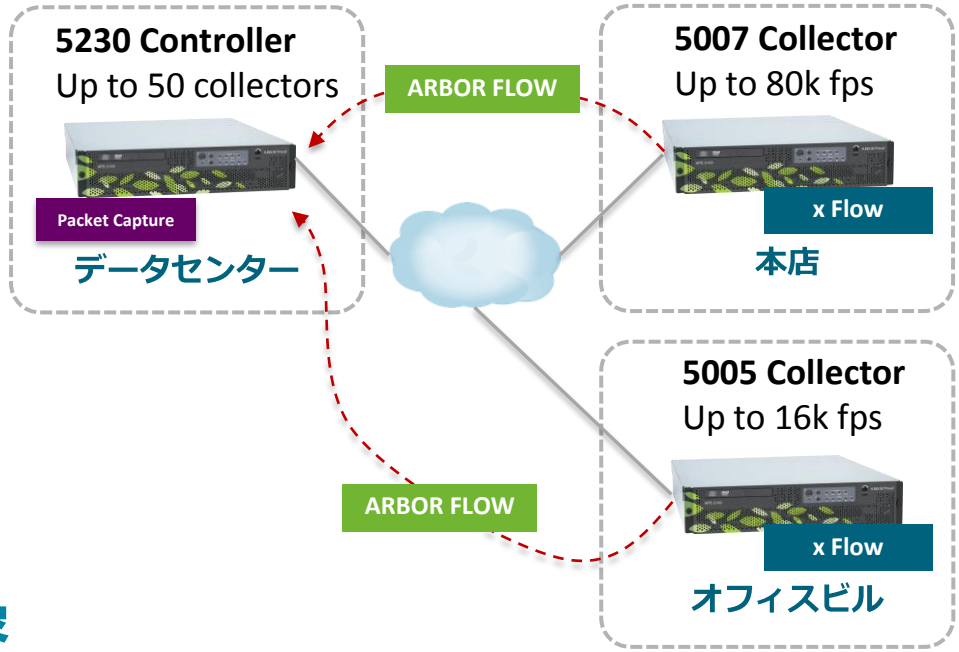
プロジェクト

- 内部からの攻撃、内部デバイス上のボット識別、不正な宛先に情報が漏洩することを防ぐ、セキュリティ・ソリューションを探しています。
  - 悪意のある活動や重要なシステムを監視・追跡を行いたい。

商談シナリオ: リモート・セールス (BYOD)

ネットワーク

- 本社(1)およびオフィスビル(12)つのオフィスビルがある。社員やお客様に有線および無線アクセスを世界中に提供しています。
- 主要ITデータセンターには、VPNでリモート・アクセスするホストが含まれています。



お見積り内容

2x 5230 + 12x 5005 + 1x 5507
メンテナンス＆サポート、ATF（年次）

プロジェクト管理、設計・構築 + トレーニング

Total ~ 機器 + サービス + /年次サポート *

* 機器およびサポート費用の価格は販売代理店にお問い合わせください。

ARBOR NETWORKS