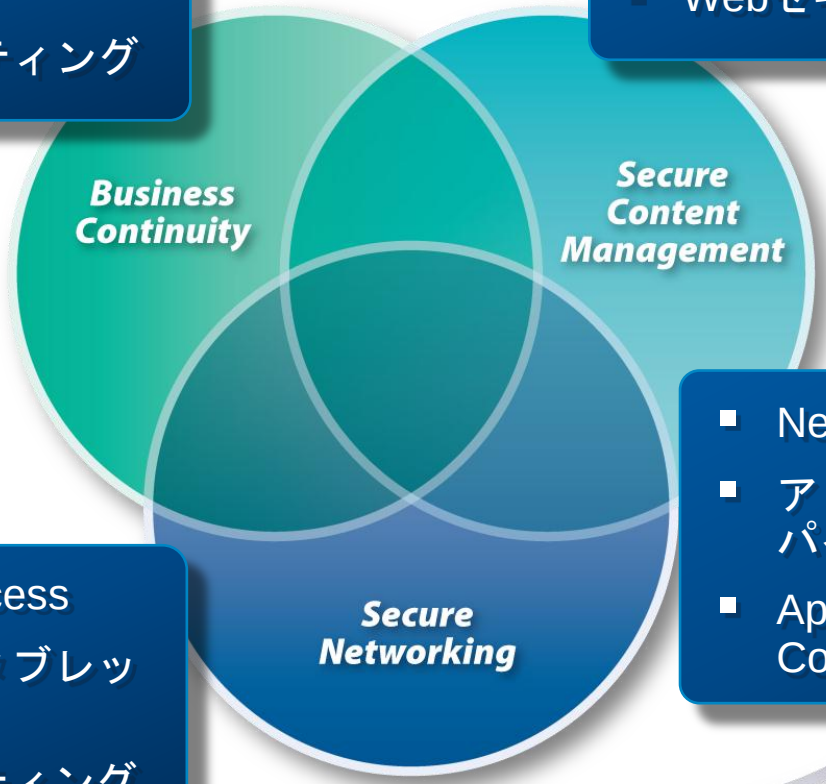
Dell SonicWALL
Next Generation Firewall & Threat Analysis

Dynamic Security for the Global Network

- 統合管理ソリューション
- モニタリング
- ロギングとレポーティング

- アンチスパム
- Emailセキュリティ
- Webセキュリティ



- Network Security（UTM）
- アンチウィルス、アンチスパイウェア、IPS
- Application Intelligence and Control

- Secure Remote Access
- スマートフォン、タブレット端末サポート
- ロギングとレポーティング

Dell SonicWALL Product Lineup

Integrated Security Solution





UTM	SSL-VPN	Email Security	CDP	Management
•TZ Series •NSA Series •E-Class NSA Series •SuperMassive Series	•SRA Series •SRA VA •Aventail Series •Aventail VA	•Email Security Series •Email Security VA	•CDP Series	•E-Class UMA •GMS •GMS VA •Analyzer
Support Service				

Next Generation Firewall

Dell SonicWALL NGFW Lineup

Enterprise/Data Center

Dell SonicWALL SuperMassive Series

SuperMassive E10800
SuperMassive E10400
SuperMassive E10200

SuperMassive 9600
SuperMassive 9400
SuperMassive 9200

Dell SonicWALL NSA Series

NSA3600
NSA4600
NSA5600
NSA6600

SMB/Campus/Branch

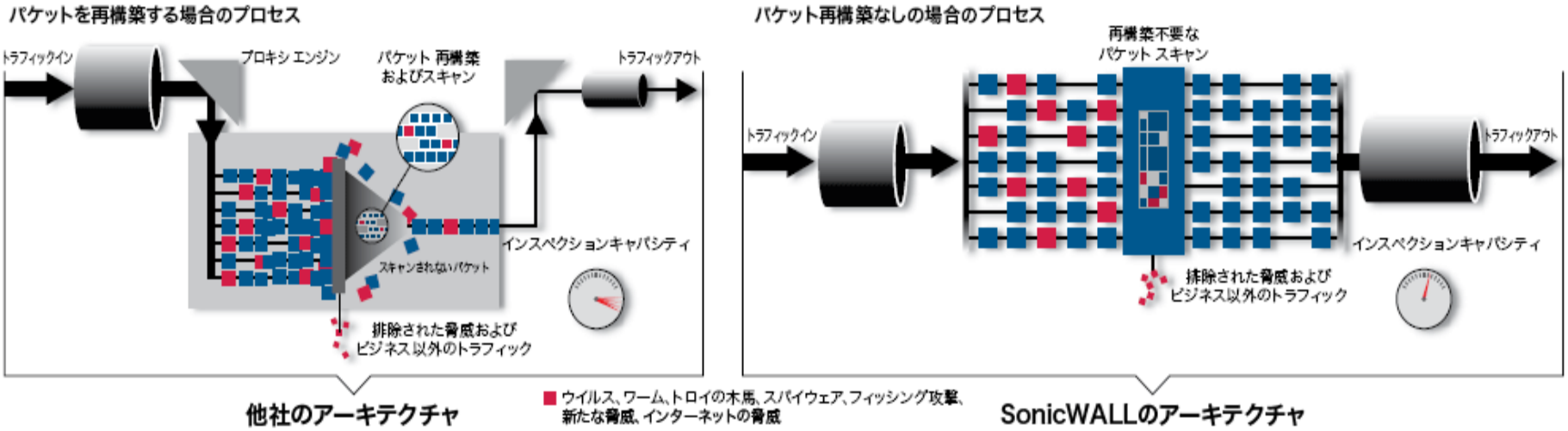
Dell SonicWALL NSA Series

NSA220W
NSA250M
NSA2400

Dell SonicWALL TZ Serie

TZ 215
TZ 205
TZ 105

先進の特許技術 - RFDPI



RFDPI（リアセンブリフリー・ディープパケットインスペクション）は、パケットの再構築を実施せずにウィルススキャンを実行する先進の技術です。

スキャン用のメモリ領域でパケットを再構築せずにスキャンする技術で、従来からある、再構築してからスキャンする手法に比べて処理速度が向上します。

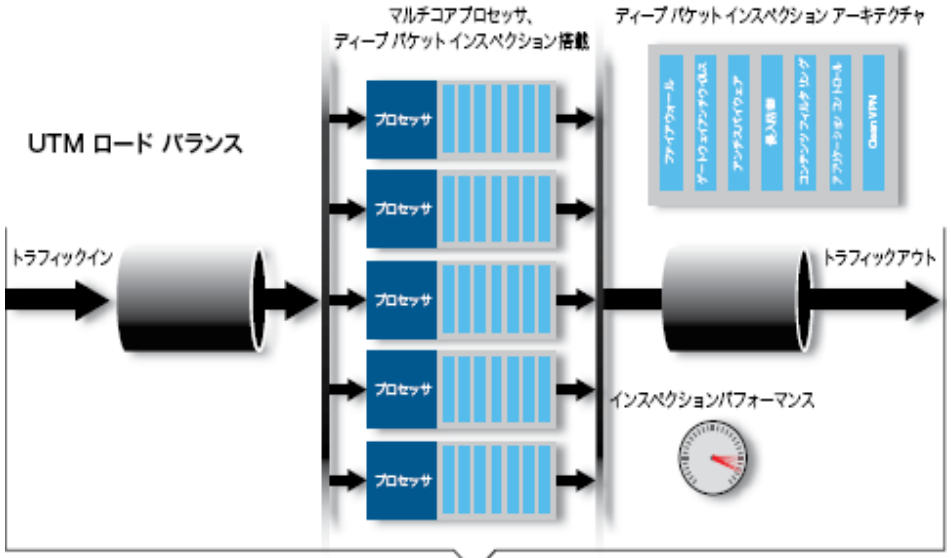
また、スキャン済みの部分を順次パケットに再分割して配信する、フロー型と呼ばれるスキャン手法とも異なり、検知率の劣化が起きません。

RFDPIは、よりセキュアで高速なネットワークを実現するために必要な技術です。

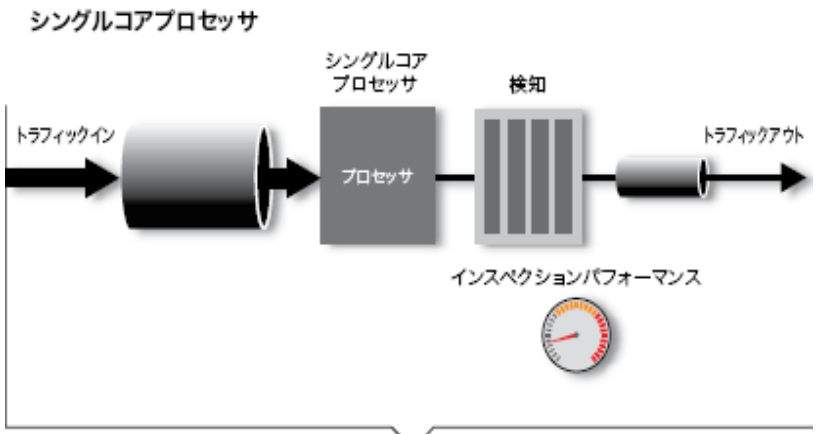
マルチコアアーキテクチャ

従来のUTMのデメリットであった、ゲートウェイアンチウィルス、IPS、URLフィルタリングといった、ファイアウォール以外の機能を利用した際のスループット低下率を最小限に留めるため、Dell SonicWALLのNGFWはマルチコアアーキテクチャを採用。

NSA6600では、24コアのネットワークCPUを搭載し、分散処理を実施。



SonicWALLのアーキテクチャ



他社のアーキテクチャ

UTM機能だけでなく、ネットワークの可視化をもスムーズに実行できるスペックを備えています。

可視化を実現するためにオーバースペックなサイジングを実施する必要がなく、費用対効果にすぐれたソリューションです。

次世代ファイアーウォール機能
Application Intelligence & Control

識別

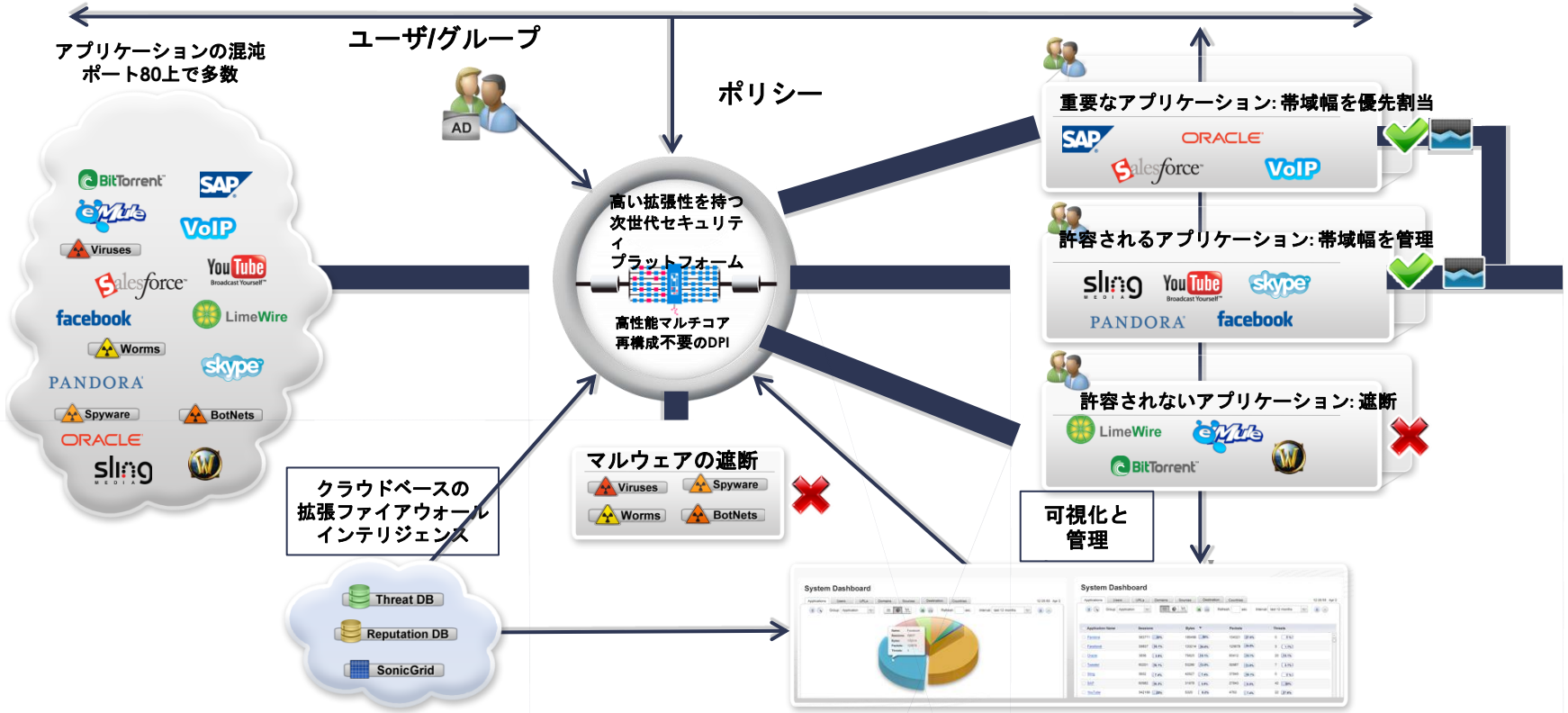
ポートやプロトコルではなくアプリケーションで
IPではなくユーザ/グループで
ファイル名ではなくコンテンツ検査で

分類

アプリケーション別
アプリケーション分類別
宛先別
コンテンツ別
ユーザ/グループ別

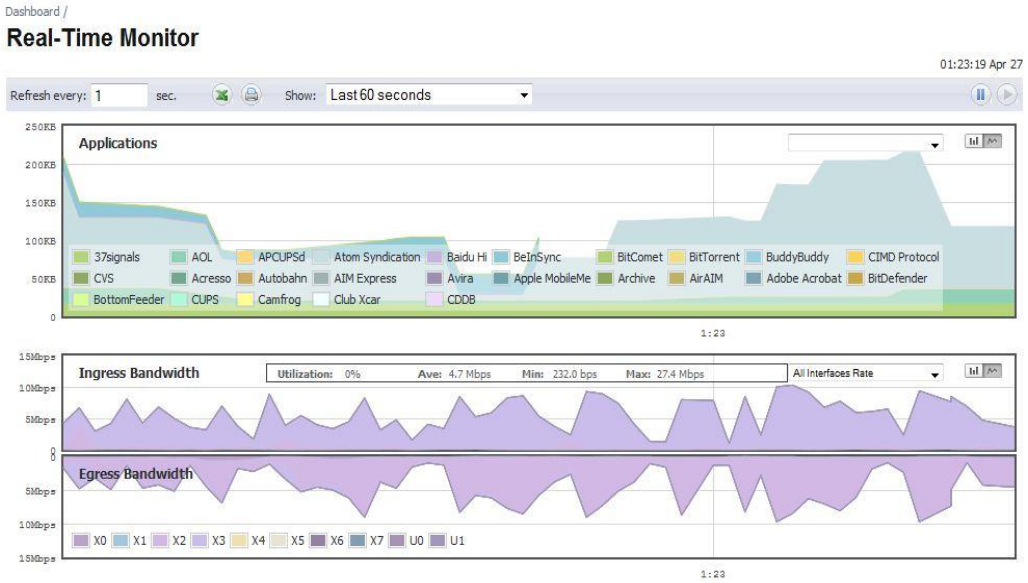
コントロール

ポリシーによるアプリケーションの優先順位設定
ポリシーによるアプリケーションの管理
ポリシーによるアプリケーションの遮断
マルウェアの検知と遮断
侵入試行の検知と防止



ネットワークの可視化

- ネットワークの可視化により、ユーザーのアクティビティを把握
- ネットワークの状態把握による投資の最適化が可能
- アプリケーション単位での帯域制御、通信制御が可能
  - 1,692種類のアプリケーションを識別可能（2012年10月22日現在）
  - カスタムシグネチャの作成も可能
  - 日本特有のアプリケーションの識別も可能
    - 宅ファイル便
    - ニコニコ動画
    - 2チャンネル
    - サイボウズ
    - デスクネッツ等



Dell SonicWALL NGFW Features

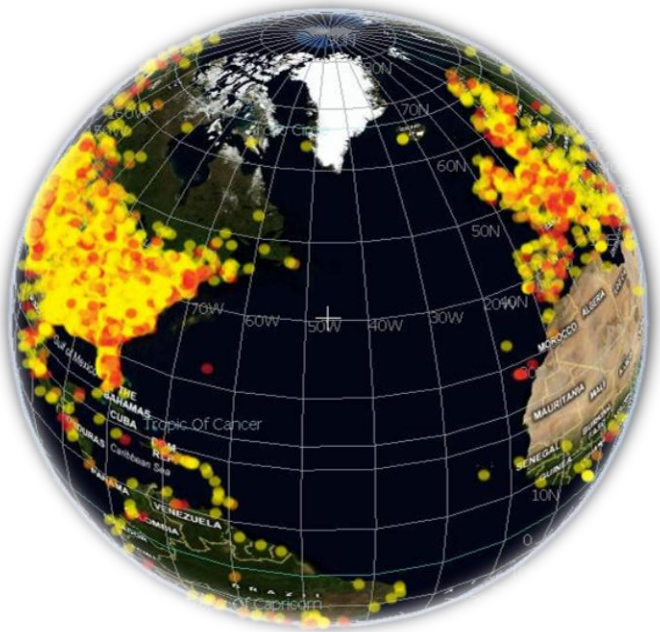
- Application Control
- IPS
- Anti-Malware
- URL Filtering
- SSL and IPSec VPN
- Bandwidth Management
- Anti-Spam
- Wireless Management
- Enforced Client Anti-Virus
- WAN Acceleration

- **マルチファンクション・セキュリティ・システム**
  - IPS、アンチマルウェア、アンチウィルス、URLフィルタリング等の統合ゲートウェイセキュリティシステム
  - セキュリティシステムの統合によるコスト削減が可能
- **ネットワークの可視化と制御**
  - 自ネットワークの状態把握による投資の最適化が可能
  - アプリケーション単位での帯域制御、通信制御が可能
- **柔軟な接続性**
  - Clean VPNソリューションの提供
  - Windows、MAC、Linux用SSL-VPNクライアントを提供
- **ネットワークの最適化**
  - WANアクセラレーション
  - トラフィックシェーピング
  - トラフィック・デデュプリケーション

Dell SonicWALL GRID Network

Dell SonicWALLは、多種多様な脅威情報の収集システムとしてGRID（Global Response Intelligent Defense）Networkを展開しています。

- 世界中の脅威を24時間365日モニタリング（100万個以上のセンサー）
- 高度な解析を用いて脅威を検知
- 業界をリードする対応性
- 予防保護
- 経験値の高い自社の専門セキュリティ調査チーム
- 主要な研究機関へ積極的に参加（WildList、AVIEN、PIRT、APWG等）
- Microsoft Active Protection Program（MAPP）のメンバー
- 各種セキュリティ機能による包括的な防御
  - IPSシグネチャ：約4,000個※
  - アンチウィルスシグネチャ：約20,000個※
  - アンチスパイウェアシグネチャ：約3,700個※
  - アプリケーション制御シグネチャ：約3,000個※
  - アプリケーションシグネチャ：約1,400個※

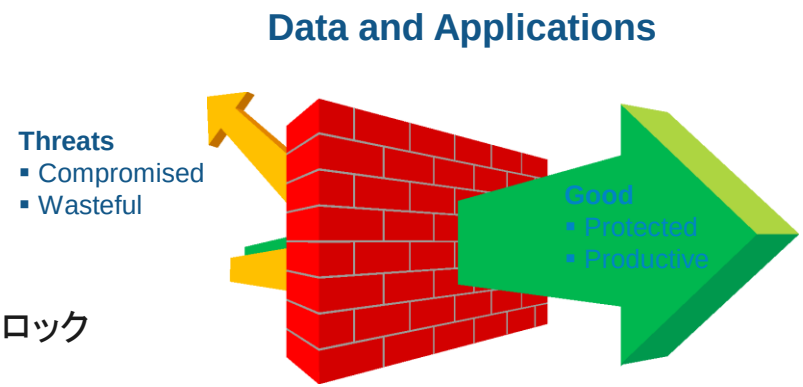


※2013年8月現在。

アンチウィルス、IPS機能

ネットワーク可視化、アンチウィルス、IPSが統合されたセキュリティ機能

- アンチウィルス、IPSシグネチャをリアルタイムに更新
- クラウドアンチウィルスの併用により、ゼロデイアタック、標的型攻撃からも保護
- キーロガー、バックドア等のスパイウェアの侵入をブロック
- ボットネットの活動を阻止
- ステートフルファイアウォールでは防ぎきれなかった脅威をブロック
- Application Intelligence and Control機能により、アプリケーションレベルでの帯域制御、アクセス制御が可能
- ネットワークの可視化により、ユーザーのアクティビティを把握



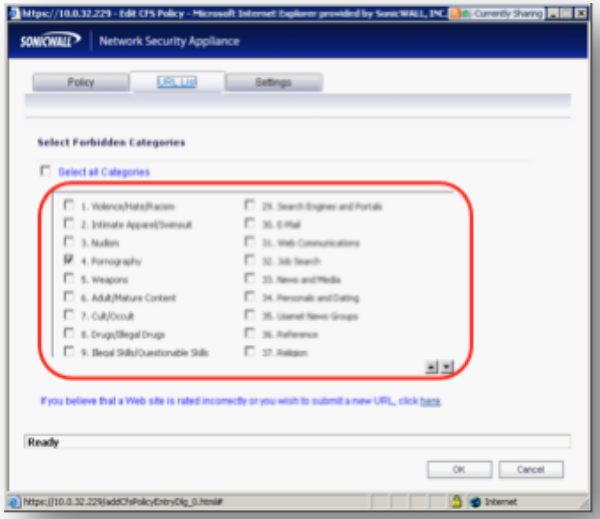
Did You Know?

パッチが提供されなくなったレガシーシステムを保護することができます！

URLフィルタリング

Content Filtering Service (CFS)

- ウィルス配布サイト等、危険なサイトへのアクセスを防止し、セキュリティレベルを向上
- 公序良俗に反するサイトへのアクセス、業務に無関係なサイトへのアクセスを防止し、生産性を向上
- 2000万サイト以上のURLデータベースを56個のカテゴリに分類
- ユーザーレベル、時間帯等を基準に柔軟なポリシーの作成が可能

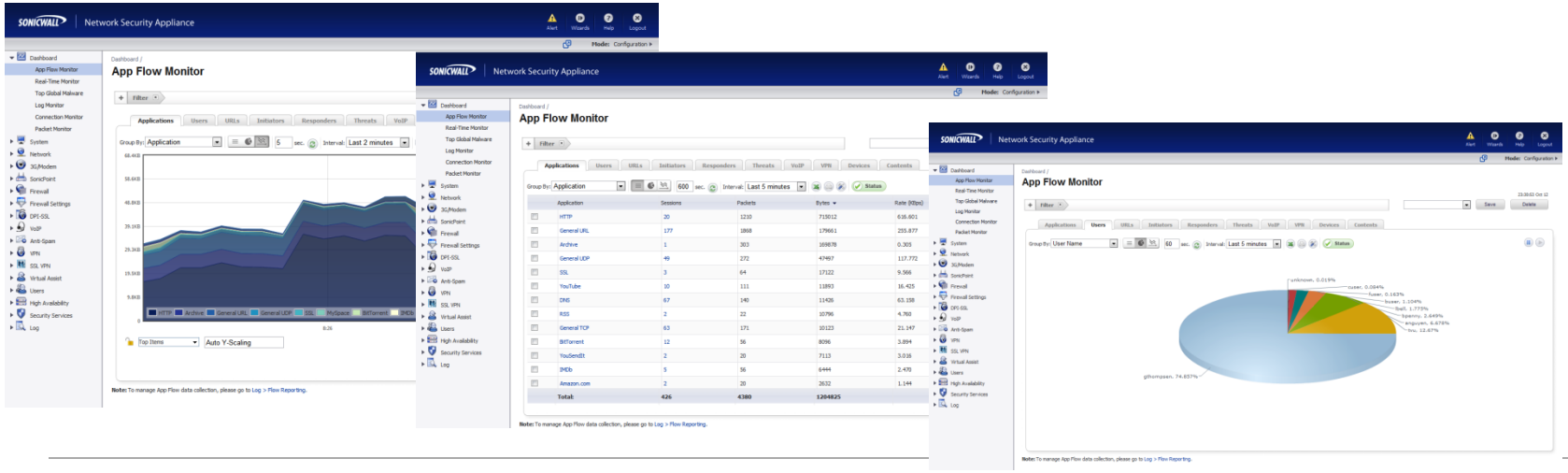


Did You Know?

標的型攻撃は、まず初めにマルウェアに感染させるために、
気づかないうちに悪意あるWebサイトにアクセスさせる手法がよく使われています。

Application Intelligence & Control

- アプリケーション、ユーザー、URL等を基準にリアルタイムでネットワークの使用状況を可視化し制御
  - *Facebookへの基本的なアクセスは許可するが、業務時間中のソーシャルゲームの利用はブロックする*
  - *チャットの利用は許可するが、チャットのファイル転送機能はブロックする*
  - *ストリーミングビデオの閲覧は帯域を10%に制限する*
  - *P2Pソフトの通信をブロックする*



Dell SonicWALL Analyzer

時系列での帯域使用レポート

SONICWALL Analyzer 7.0

SonicToday | UTM | SRA | CDP | Console | Try GMS Free 30 Days | Help | Logout

CARMEL NSA E-6500 - GOOD FOR REPORTS! :: Timeline

User: demo@LocalDomain | Guest Users

ModelView
- Model : NSA 240 Expanded
  - DAISY - NSA 240 BACKUP
- Model : NSA E6500
  - CARMEL NSA E-6500 - G
- Model : NSA E8500
  - TAHOE - NSA E-8500 HA

- General
- Data Usage
- Applications
  - Data Usage
  - Detected
  - Blocked
  - Categories
  - Initiators
  - Timeline
- Web Activity
- Web Filter
- VPN Usage
- Intrusions
- GAV
- Anti-Spyware
- Attacks
- Authentication

タイムライン　8月 01, 2012 00:00 終了日 8月 31, 2012 23:59

- Load Custom Report -

タイムライン

1,800,000 / 1,600,000 / 1,400,000 / 1,200,000 / 1,000,000 / 800,000 / 600,000

3,000,000,000 / 2,500,000,000 / 2,000,000,000 / 1,500,000,000 / 1,000,000,000 / 500,000,000 / 0

2012/... 2012/... 2012/... 2012/... 2012/...

イベント
転送済み

		イベント	転送済み
		1,061,374	395.92 MB
		1,148,513	458.3 MB
		1,049,127	428.58 MB
		1,143,671	385.94 MB
		1,112,901	352.74 MB
		1,194,989	895.13 MB
		1,112,127	373.8 MB
8	2012/08/08	1,724,629	1.38 GB
9	2012/08/09	1,618,024	1.46 GB
10	2012/08/10	1,517,317	1.36 GB
11	2012/08/11	1,350,670	2.36 GB
12	2012/08/12	1,576,484	1.38 GB
13	2012/08/13	1,656,562	1.07 GB
14	2012/08/14	1,310,903	1.41 GB
15	2012/08/15	1,631,131	2.57 GB

インシデント発生時やトラフィックのバーストを発見し、該当する時間帯の棒グラフをクリックして、当該時間帯の詳細をドリルダウンして調査することが可能。

トラフィックバースト時の詳細情報にドリルダウン

SONICWALL Analyzer 7.0

SonicToday | UTM | SRA | CDP | Console | Try GMS Free 30 Days | Help | Logout

CARMEL NSA E-650

User: demo@LocalDomain | Guest Users

P2Pの通信があることが判明。
これをクリックして、具体的に、アプリケーション名、送信元、送信先を特定する。

ModelView
- Model : NSA 240 Expanded
  - DAISY - NSA 240 BACKUP
- Model : NSA E6500
  - CARMEL NSA E-6500 - G
- Model : NSA E8500
  - TAHOE - NSA E-8500 HA

- General
- Data Usage
- Applications
  - Data Usage
  - Detected
  - Blocked
  - Categories
  - Initiators
  - Timeline
- Web Activity
- Web Filter
- VPN Usage
- Intrusions
- GAV
- Anti-Spyware
- Attacks
- Authentication
- Analyzers
- Configuration
- Events
- Custom Reports

アプリケーシ

了日 8月 15, 2012 23:59

- Load Custom Report -

タイムライン

90,000 / 80,000 / 70,000 / 60,000 / 50,000 / 40,000 / 30,000 / 20,000

250,000,000 / 200,000,000 / 150,000,000 / 100,000,000 / 50,000,000 / 0

4:00 / 8:00 / 12:00 / 16:00 / 20:00

イベント / 転送済み

カテゴリ

	アプリケーション カテゴリ	イベント	転送済み
1	PROTOCOLS	575,847	2.15 GB
2	P2P	931,080	240.95 MB
3	MULTIMEDIA	99,948	65.82 MB
4	REMOTE-ACCESS	2,602	46.98 MB
5	SOCIAL-NETWORKING	7,837	29.73 MB
	合計	1,617,314	2.53 GB

アプリケーション

	アプリケーション	脅威レベル	イベント	転送済み
1	BitTorrent/uTorrent	GUARDED	850,115	235.27 MB
2	HTTP	GUARDED	445,741	2.14 GB

さらにドリルダウン

使用されたアプリケーション、送信元IPアドレス、宛先IPアドレスが判明。
ユーザ認証を実施している場合は、ユーザー名も判明するため、当該PC及び当該ユーザーを調査する必要がある。

SONICWALL Analyzer 7.0

SonicToday | UTM | Help | Logout

CARMEL NSA E-6500 - GOOD FOR REPORTS! :: Timeline

ModelView
- Model : NSA 240 Expanded
  - DAISY - NSA 240 BACKUP
- Model : NSA E6500
  - CARMEL NSA E-6500 - G
- Model : NSA E8500
  - TAHOE - NSA E-8500 HA

- General
- Data Usage
- Applications
  - Data Usage
  - Detected
  - Blocked
  - Categories
  - Initiators
  - Timeline
- Web Activity
- Web Filter
- VPN Usage
- Intrusions
- GAV
- Anti-Spyware
- Attacks
- Authentication
- Analyzers
- Configuration
- Events
- Custom Reports

アプリケーションの詳細

アプリケーション カテゴリ = P2P

アプリケーション

	アプリケーション	脅威レベル	イベント	転送済み
1	BitTorrent/uTorrent	GUARDED	850,115	235.27 MB
2	eMule	GUARDED	79,983	5.65 MB
3	GNUTella	HIGH	798	24.78 KB
4	PP	HIGH	71	1.62 KB
5	LimeWire	SEVERE	48	0 B
	合計		931,015	240.95 MB

始動者

	始動者 IP	始動者のホスト	ユーザ	イベント	転送済み
1	172.30.170.138	ceastwood-pc.complab.eng	COMPLAB\ceastwood	348,854	119.17 MB
2	172.30.170.133	fdurant-pc.complab.eng	COMPLAB\fdurant	258,322	111.86 MB
3	172.30.170.137	cbronson-pc.complab.eng	COMPLAB\cbronson	77,233	5.46 MB
4	172.30.170.138		COMPLAB\ceastwood	11,999	3.05 MB
5	172.30.170.133		COMPLAB\fdurant	3,777	1.17 MB
	合計			700,185	240.7 MB

応答者

	応答者 IP	応答者のホスト	イベント	転送済み
1	172.30.170.138	ceastwood-pc.complab.eng	199,161	0 B
2	172.30.170.133	fdurant-pc.complab.eng	20,617	0 B
3	172.30.170.138		7,383	0 B

宛先Webサイト毎の帯域使用レポート

Webサイトのカテゴリ毎のアクセス履歴をグラフ化。
ポリシー違反サイトのカテゴリをクリックして、送信元及び宛先を特定。

SONICWALL Analyzer 7.0

SonicToday | UTM | SRA

Help | Logout

CARMEL NSA E-6500 - GOOD FOR REPORTS! :: Categories

LocalDomain | Guest Users

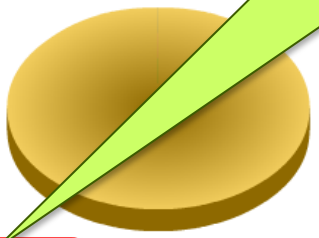
- ModelView
  - Model : NSA 240 Expanded
    - DAISY - NSA 240 BACKUP
  - Model : NSA E6500
    - CARMEL NSA E-6500 - G
  - Model : NSA E8500
    - TAHOE - NSA E-8500 HA

- General
- Data Usage
- Applications
- Web Activity
- Web Filter
  - Categories
  - Sites
  - Initiators
  - Timeline
  - Details
- VPN Usage
- Intrusions
- GAV
- Anti-Spyware
- Attacks
- Authentication
- Analyzers
- Configuration
- Events
- Custom Reports

トップ カテゴリ

- Load Custom Report -

カテゴリ



- Administrative Custom List settings
- Weapons
- Adult/Mature Content
- Intimate Apparel/Swimsuit
- Pornography
- Drugs/Illegal Drugs
- Cult/Occult

	カテゴリ	試行
1	Administrative Custom List settings	888,076
2	Weapons	307
3	Adult/Mature Content	153
4	Intimate Apparel/Swimsuit	98
5	Pornography	52
6	Drugs/Illegal Drugs	9
7	Cult/Occult	3
	合計	888,698

• レポートが生成されたタイムゾーン: Pacific Standard Time
• Report owner: System@LocalDomain

ポリシー違反サイトへのアクセス者を特定

SONICWALL Analyzer 7.0

SonicToday | UTM | SRA | CDP | Console | Try GMS Free 30 Days | Help | Logout

CARMEL NSA E-6500 - GOOD FOR REPORTS! :: Categories

User: demo@LocalDomain | Guest Users

ModelView
- Model : NSA 240 Expanded
  - DAISY – NSA 240 BACKUP
- Model : NSA E6500
  - CARMEL NSA E-6500 – G
- Model : NSA E8500
  - TAHOE – NSA E-8500 HA

- General
- Data Usage
- Applications
- Web Activity
- Web Filter
  - Categories
  - Sites
  - Initiators
  - Timeline
  - Details
- VPN Usage
- Intrusions
- GAV
- Anti-Spyware
- Attacks
- Authentication
- Analyzers
- Configuration
- Events
- Custom Reports

ウェブ フィルタの詳細

カテゴリ = Adult/Mature Content

Custom Report -

宛先URLとアクセス者が判明。

サイト

	サイト IP	サイト名	カテ	
1	50.97.143.30	fuckmelikethat.tumblr.com	Adult/Matu	27
2	50.97.143.25	fuckmelikethat.tumblr.com	Ad ent	19
3	50.97.151.194	fuckmelikethat.tumblr.com	ature Content	19
4	50.97.143.26	fuckmelikethat.tumblr.com	Adult/Mature Content	13
5	50.97.151.201	fuckmelikethat.tumb	Adult/Mature Content	12
	合計			90

始動者

	始動者 IP	始動者のホスト	ユーザ	試行
1	172.30.170.140	mpark-pc.complab.eng	COMPLAB\mparkinson	65
2	172.30.130.134	smacintosh-pc.complab.eng	COMPLAB\smacintosh	48
3	172.30.130.134		COMPLAB\smacintosh	21
4	172.30.170.140		COMPLAB\mparkinson	19
	合計			153

始動者の国

	始動者の国	試行
1	Private IP	153
	合計	153

応答者の国

IPSの検知レポート

SONICWALL Analyzer 7.0

SonicToday | UTM | SRA | CDP | Console | Try GMS Free 30 Days | Help | Logout

CARMEL NSA E-6500 - GOOD FOR REPORTS! :: Detected

User: demo@LocalDomain | Guest Users

- ModelView
  - Model : NSA 240 Expanded
    - DAISY - NSA 240 BACKUP
  - Model : NSA E6500
    - CARMEL NSA E-6500 - G
  - Model : NSA E8500
    - TAHOE - NSA E-8500 HA

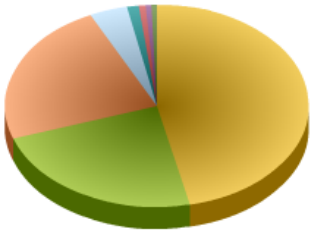
- General
- Data Usage
- Applications
- Web Activity
- Web Filter
- VPN Usage
- Intrusions
  - Detected
  - Blocked
  - Targets
  - Initiators
  - Timeline
- GAV
- Anti-Spyware
- Attacks
- Authentication
- Analyzers
- Configuration
- Events
- Custom Reports

トップ侵入検知

8月 01, 2012 00:00 終了日 8月 31, 2012 23:59

- Load Custom Report -

侵入



	侵入	危険度	イベント
1	PING L3retriever	LOW	7,565
2	PING Microsoft Windows 2	LOW	3,783
3	Echo Reply	LOW	3,752
4	8327		653
5	8329		205
6	8330		115
7	8251		103
8	8169		51
9	Fragment Reassembly Time Exceeded	LOW	16
10	8326		15
11	8558		6
12	8176		3
13	8253		2
	合計		16,269

IPSのブロックレポート

注意すべき攻撃をクリックして、
攻撃元及びターゲットを特定。

SONICWALL Analyzer 7.0

SonicToday | UTM | SRA | CDP | Console | Try GMS Free 30 Days | Help | Logout

CARMEL NSA E-6500 - GOOD FOR REPORTS! :: Blocked

User: demo@LocalDomain | Guest Users

ModelView
- Model : NSA 240 Expanded
  - DAISY - NSA 240 BACKUP
- Model : NSA E6500
  - CARMEL NSA E-6500 - G
- Model : NSA E8500
  - TAHOE - NSA E-8500 HA

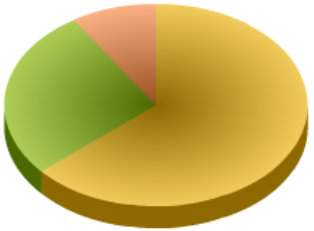
- General
- Data Usage
- Applications
- Web Activity
- Web Filter
- VPN Usage
- Intrusions
  - Detected
  - Blocked
  - Targets
  - Initiators
  - Timeline
- GAV
- Anti-Spyware
- Attacks
- Authentication
- Analyzers
- Configuration
- Events
- Custom Reports

トップ侵入遮断

8月 01, 2012 00:00 終了日 8月 31, 2012 23:59

- Load Custom Report -

侵入



	侵入	危険度	イベント
1	Suspicious HTTP Content-Length Header 11 (Negative Value)	MEDIUM	14
2	HTTP Server Shellcode Exploit 5	MEDIUM	6
3	7833		2
	合計		22

• レポートが生成されたタイムゾーン: Pacific Standard Time
• Report owner: System@LocalDomain

IPSブロックレポートのドリルダウン

SONICWALL Analyzer 7.0

SonicToday | UTM | SRA

Help | Logout

CARMEL NSA E-6500 - GOOD FOR REPORTS! :: Blocked

@LocalDomain | Guest Users

ModelView
- Model : NSA 240 Expanded
  - DAISY - NSA 240 BACKUP
- Model : NSA E6500
  - CARMEL NSA E-6500 - G
- Model : NSA E8500
  - TAHOE - NSA E-8500 HA

- General
- Data Usage
- Applications
- Web Activity
- Web Filter
- VPN Usage
- Intrusions
  - Detected
  - Blocked
  - Targets
  - Initiators
  - Timeline
- GAV
- Anti-Spyware
- Attacks
- Authentication
- Analyzers
- Configuration
- Events
- Custom Reports

侵入の詳細

侵入 = HTTP Server Shellcode Exploit 5

Custom Report -

侵入

	侵入	危	イベント
1	HTTP Server Shellcode Exploit 5		6
	合計		6

侵入種別

	侵入種別	イベント
1	EXPLOIT	6
	合計	6

ターゲット

	ターゲット IP	ターゲット	イベント
1	173.223.232.113		3
2	173.223.232.131		3
	合計		6

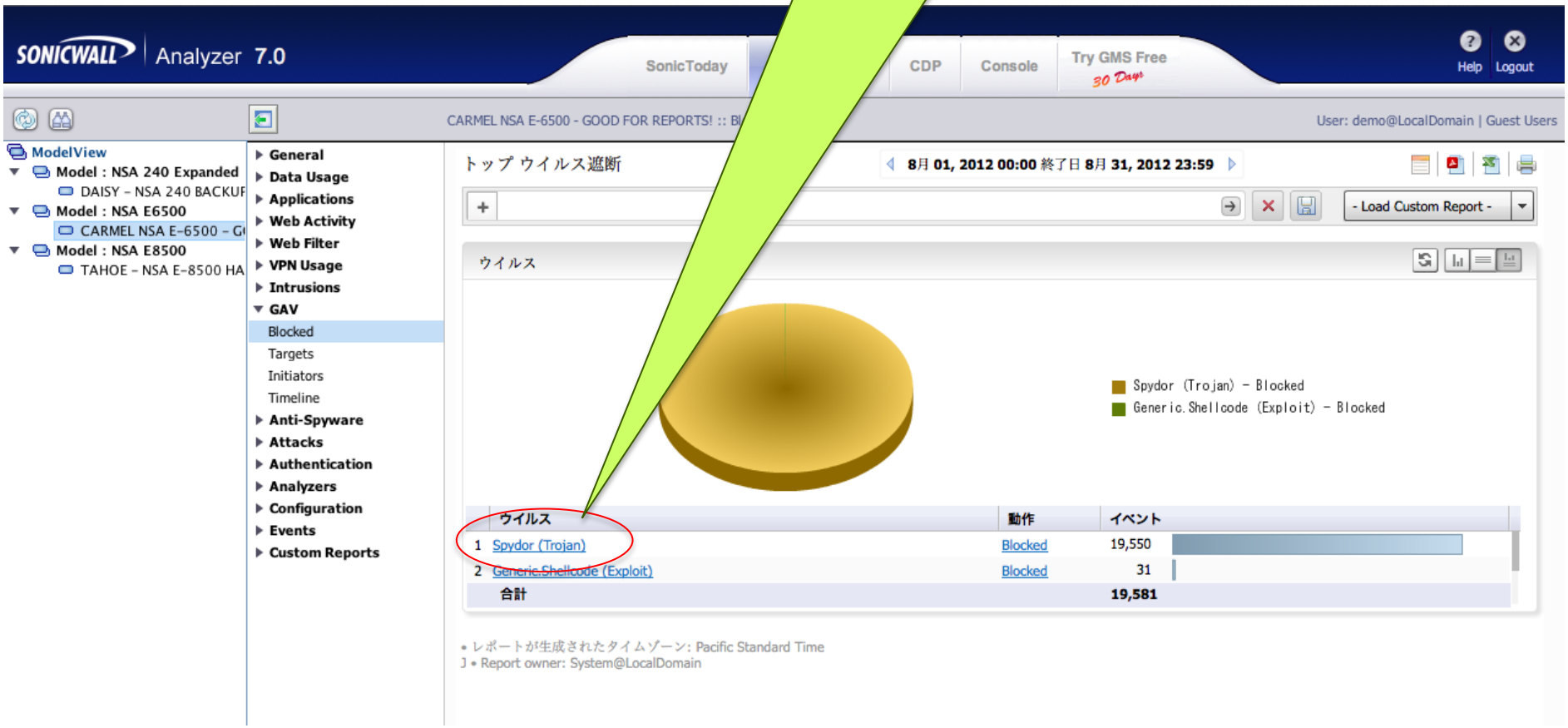
始動者

	始動者 IP	始動者のホスト	ユーザ	イベント
1	172.30.170.132		COMPLAB\pcornwall	3
2	172.30.170.132	pcornwall-pc.complab.eng	COMPLAB\pcornwall	3
	合計			6

攻撃のターゲットと攻撃者が判明し、さらに攻撃者が社内にいることが判明。
自社が加害者になってしまっている可能性があるため、早急な調査と対策が必要。

ウィルスの検知レポート

当該ウィルスパケットの送信元と宛先を特定。



ウィルス検知レポートのドリルダウン

ウィルスパケットの宛先とウィルスの送信元が判明。
ターゲットが社内になっているため、当該PCの調査、確認が必要。

SONICWALL Analyzer 7.0

SonicToday

Help Logout

CARMEL NSA E-6500 - GOOD FOR REPORTS! :: Blocked

User: demo@LocalDomain | Guest Users

ModelView
- Model : NSA 240 Expanded
  - DAISY – NSA 240 BACKUP
- Model : NSA E6500
  - CARMEL NSA E-6500 – G
- Model : NSA E8500
  - TAHOE – NSA E-8500 HA

General
Data Usage
Applications
Web Activity
Web Filter
VPN Usage
Intrusions
GAV
- Blocked
- Targets
- Initiators
- Timeline

Anti-Spyware
Attacks
Authentication
Analyzers
Configuration
Events
Custom Reports

ウイルスの詳細

ウイルス = Spydor (Trojan)

- Load Custom Report -

ウイルス

	ウイルス	動作	イベント
1	Spydor (Trojan)	Blocked	4,608
	合計		4,608

ターゲット

	ターゲット IP	ターゲットホスト	イベント
1	172.30.170.128	dm[illegible]pc.complab.eng	3,287
2	172.30.170.128		1,321
	合計		4,608

始動者

	始動者 IP	始動者のホスト	ユーザ	イベント
1	173.240.215.101			4,608
	合計			4,608

対象国

	対象国	イベント
1	Private IP	4,608
	合計	4,608

ファイアーウォールでの攻撃検知レポート

SONICWALL Analyzer 7.0

SonicToday | UTM | SRA | CDP | Console | Try GMS Free 30 Days | Help | Logout

CARMEL NSA E-6500 - GOOD FOR REPORTS! :: Attempts

User: demo@LocalDomain | Guest Users

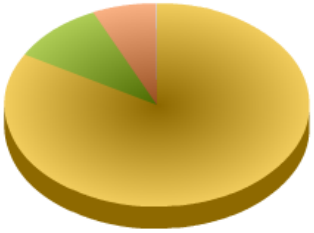
- ModelView
  - Model : NSA 240 Expanded
    - DAISY - NSA 240 BACKUP
  - Model : NSA E6500
    - CARMEL NSA E-6500 - G
  - Model : NSA E8500
    - TAHOE - NSA E-8500 HA

- General
- Data Usage
- Applications
- Web Activity
- Web Filter
- VPN Usage
- Intrusions
- GAV
- Anti-Spyware
- Attacks
  - Attempts
  - Targets
  - Initiators
  - Timeline
- Authentication
- Analyzers
- Configuration
- Events

トップ試行　9月 01, 2012 00:00 終了日 9月 07, 2012 23:59

- Load Custom Report -

攻撃



	攻撃	イベント
1	TCP connection dropped	1,925,763
2	Web access request dropped	228,287
3	ICMP packet dropped due to policy	156,757
4	TCP Syn/Fin packet dropped	1,863
5	Smurf Amplification attack dropped	123
6	Possible port scan detected	38
7	IP spoof dropped	15
8	FTP: PASV response bounce attack dropped.	12
9	TCP Xmas Tree dropped	8
10	Probable TCP NULL scan detected	4
	合計	2,312,870

• レポートが生成されたタイムゾーン: Pacific Standard Time
• Report owner: System@LocalDomain

特定の攻撃をクリックして、
その詳細にドリルダウン。

Thank you