

2008/01/01

SecureSoft SNIPER IPS White Paper

アプライアンス製品

1. IPS とは

IPSとは Intrusion Prevention System の略で、ネットワーク上の不正アクセスの検知・防御を能動的に行い、自動で解決案を出せるソリューションです。ネットワークの遅延を最小化してネットワークの切断を発生しないことが大前提となります。

1.1 Gartner Group の IPS の正義

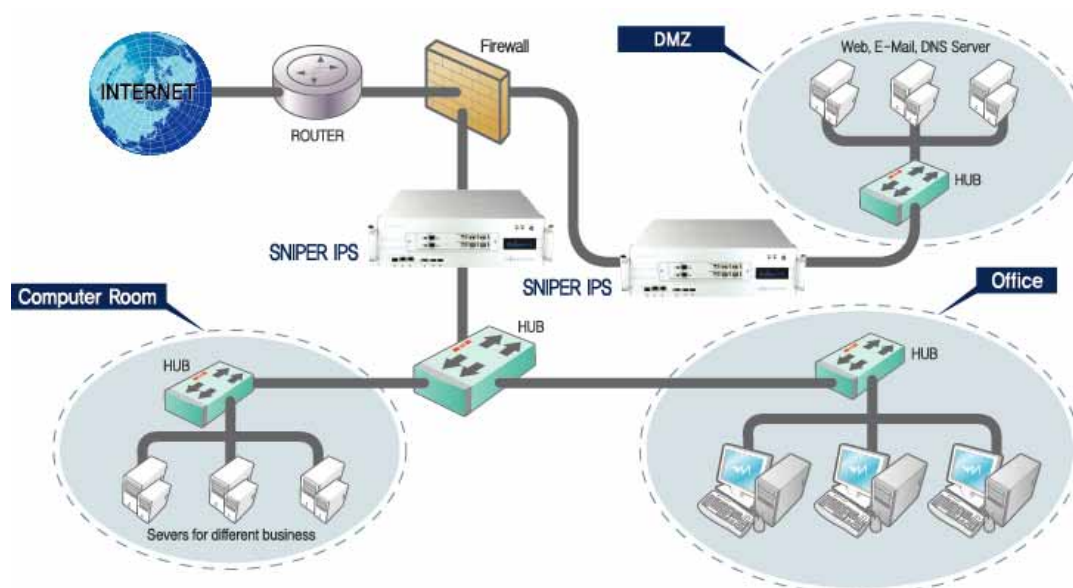
米国の Gartner Group は下記のように IPS というソリューションを正義しました。

- 防御能力と 素早い反応(High-Speed)のために In-Line に位置された製品であること
- セッションベースの検知(Session Aware Inspection)のサポートすること
- 多様なブロッキング方法(Signature, Protocol Anomaly, Action)によって悪意を持つセッション(Malicious Session)をブロッキングすること

SNIPER-IPS は上記要件をすべて揃えています。

2. SecureSoft SNIPER IPS の紹介

SNIPER-IPS はネットワーク上で発生するハッキングに対する脅威を検知、防御します。ワームやウイルスのような有害トラフィックを適切にブロッキングすることによってネットワークの信頼性と安定性を保障します。また、コンピュータシステムに対して改ざん、誤用等の行為をリアルタイムで検知、遮断して管理者へ警報することにより、内部情報の漏洩を監視および遮断することができます。



2. SecureSoft SNIPER IPS の特長

2.1 ダイナミックなルールの適用

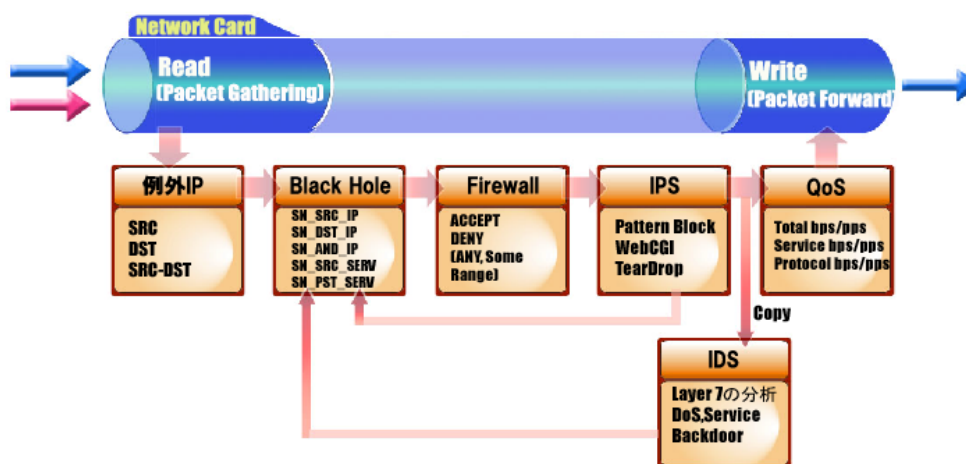
SNIPER-IPS はリアルタイムで検知した不正アクセスに対してダイナミックなルールを適用して防御することができます。即ち、検知した攻撃に対して一定な時間(秒単位)を決めてブロッキングポリシーを適用することが可能です。

2.3 SNIPER X ドライバ

SNIPER-IPS ではネットワーク上に流れているパケットを採取するために独自の技術である SNIPER-X ドライバを搭載しております。これによって、パケットの採取能力をアップしてネットワークの遅延を最小化することが可能になりました。

2.2 ALSI (Application Layer Stateful Inspection) エンジンの搭載

SNIPER-IPS で採取したパケットを ALSI エンジンでパケットの状態をレイヤー 7 まで分析します。分析する際にはシグネチャデータとマッチングしながら攻撃がどうかを判定します。このエンジンではパケットベース(One-Way)およびセッションベース(Two-Way)の攻撃まで検知・防御の処理を同時に行うことを実現しています。また、TCP Connection-Oriented ベースの攻撃を精度の高いセッション組合技術で検知、防御します。



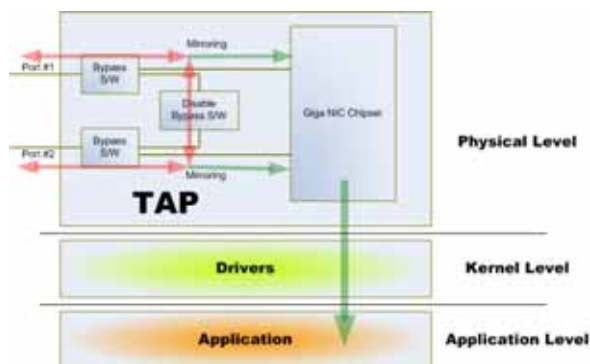
| 区分 | 内容 | 備考 |
|------------|--|----|
| 例外 IP | IP レベルで検知・防御の処理を例外として管理します。 - SRC : 攻撃元 - DST : 攻撃対象 - SRC-DST : 攻撃元と攻撃対象を同時にチェックします。 | |
| Black Hole | 実際にブロッキングされるリストを管理します。 | |

| | | |
|----------|---|--|
| | <ul style="list-style-type: none"> - SN_SRC_IP : 攻撃元(全てのサービス) - SN_DST_IP : 攻撃対象(全てのサービス) - SN_AND_IP : 攻撃元と攻撃対象を同時にチェックします。(1:1) - SN_SRC_SERV : 攻撃元、対象サービス(1:N) - SN_DST_SERV : 攻撃対象、対象サービス(N:1) | |
| Firewall | IP Range、ポートごとに ACCEPT, DROP の処理を行います。 | |
| IPS | <p>パケットの Layer4 + Payload 情報を検査します。</p> <ul style="list-style-type: none"> - Pattern Block ワーム系の攻撃に対して Pattern Matching します。 - WebCGI Web サービスに対して Pattern Matching します。 | |
| IDS | <p>パケットの L7 までの分析して複雑な攻撃に対応します。</p> <p>DoS、Service 攻撃、Backdoor 攻撃などに対応します。</p> | |
| QoS | トラフィックの閾値をプロトコル、サービスごとにかけて超過したトラフィックを DROP させます。 | |

Firewall と QoS のエンジンは ON/OFF 可能です。

IPS エンジンを無効にして IDS として運用することも可能です。

2.3 Fail Over Device



SNIPER-IPS はインラインモードで運用されるため、このシステムに障害が発生したらネットワークに影響を与えてしまい、正常なサービスができなくなる場合があります。このような問題を回避するために Fail Over Device というデバイスを LAN カードに内蔵し、システムに障害があっても迂回できる機能を提供しています。

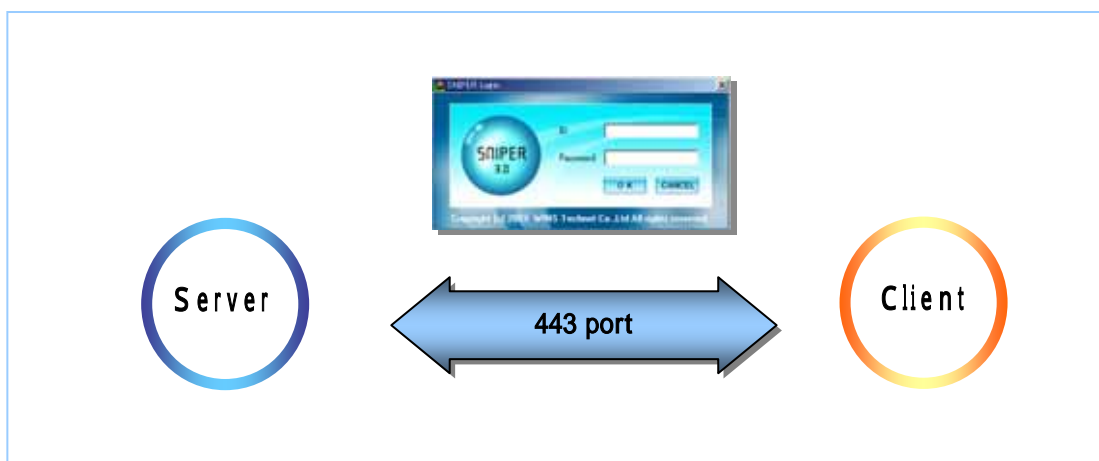
SNIPER-IPS は In-Line、SPAN、Bypass モードに切り替えることが可能です。SPAN モードの場合は通常の Bypass モードと同じく、IDS としてネットワークトラフィックをモニタリングするためにパケットをミラーリングする状況です。

2.4 Anomalyの検知

SNIPER-IPS はネットワークトラフィックのトレンドを分析する際に DoS、DDoS などの攻撃が発生したら 1 分単位でトラフィックを分析したデータを基にしてイベントを発生することができます。そして自動または手動で設定することも可能です。

2.5 ウェブベースの管理

暗号通信ポート(443)を使って SNIPER-IPS に接続してモニタリングからコンフィギュレーションまでできます。しかも、SNIPER-IPS に接続可能な管理者の IP アドレスを指定して運用することも可能です。



2.6 False Positive の最小化

SNIPER-IPS では False Positive を最小化するために次のようなメカニズムで運用されています。

- 内部・外部のネットワークを設定することによってネットワークの状況を正確に切り分けることができます。
- Raw データをキャプチャすることによって管理者はパケットの情報を正確に確認することができます。(Hacking Proof)
- 例外設定機能を使うことによって正常なネットワークポイントを検知しないようにすることができます。
- 一つの攻撃を検知する際に回数、時間を管理者がチューニングすることができます。
- 新たな攻撃に対して管理者は任意の検知ポリシーを登録することができます。

2.7 ライブアップデート

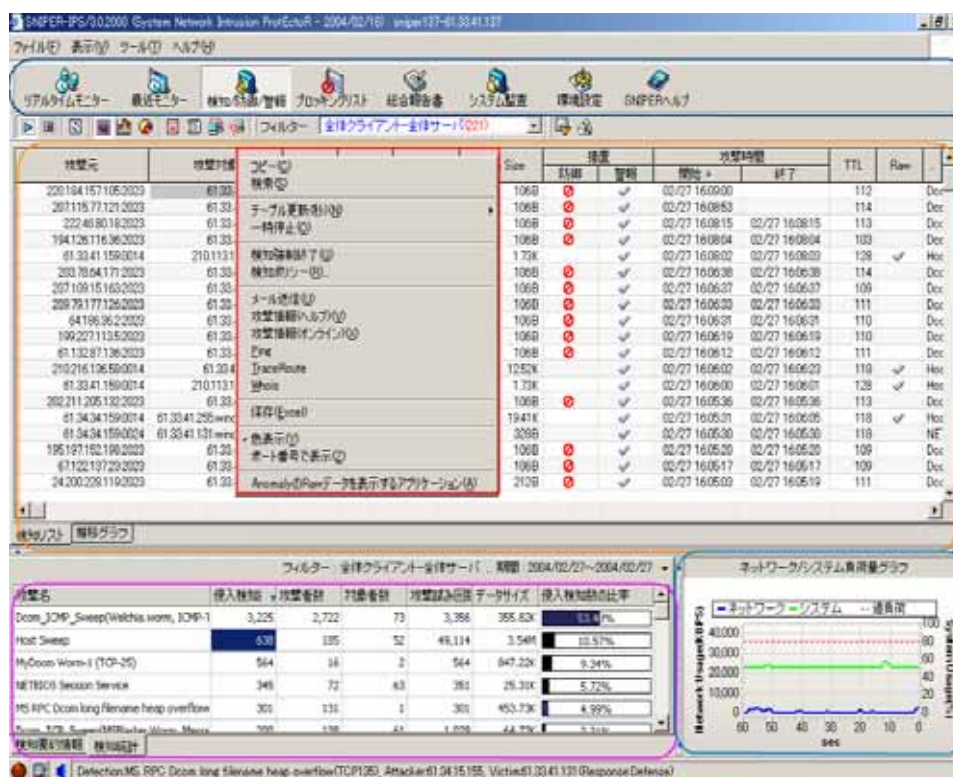


次々登場する新たな攻撃に対応するために独自の CERT チームを組んで SNIPER-IPS のお客様がすぐ対応できるようにライブアップデートを提供しています。

定期的なライブアップデートとともに致命的な攻撃が発生したら 24 時間以内に対応できるシステムを構築しています。

2.8 All-In-One Display

すべてのインタフェースを日本語化して色々な状況を一目でわかるようにしています。



3. SNIPER IPS のインタフェース

3.1 検知/防御/警報

SNIPER-IPS が検知した攻撃(Worm, DoS, Hacking 等)をリアルタイムで表示します。攻撃に対する攻撃元、攻撃対象、ポート、プロトコル、開始及び終了時間などが表示されます。また、攻撃に対して管理者が設定したその結果(検知、防御)も確認することができます。テーブルのデータはグラフ化して確認することも可能です。

3.2 ブロッキングリスト

SNIPER-IPS がブロッキングしたその履歴をリアルタイムで表示します。自動に設定したブロッキング情報または管理者が手動で設定したブロッキング情報が表示されます。その内容としてはブロッキングする時間、開始時間、満了時間、攻撃元、攻撃対象などの情報が表示されます。

3.3 リアルタイムモニター

SNIPER-IPS を経由するすべてのネットワークトラフィックの情報(サーバ、クライアント、IP アドレス等)をテーブル上に表示します。リアルタイムで表示されるデータはグラフ化して確認することもできます。

3.4 総合報告書

SNIPER-IPS が収集したデータをデータベースとして管理する機能です。データは暗号化されたバイナリコードのファイルで保存しています。リアルタイムで検知した情報を素早く保存、照会することが可能になります。

3.5 システム監査

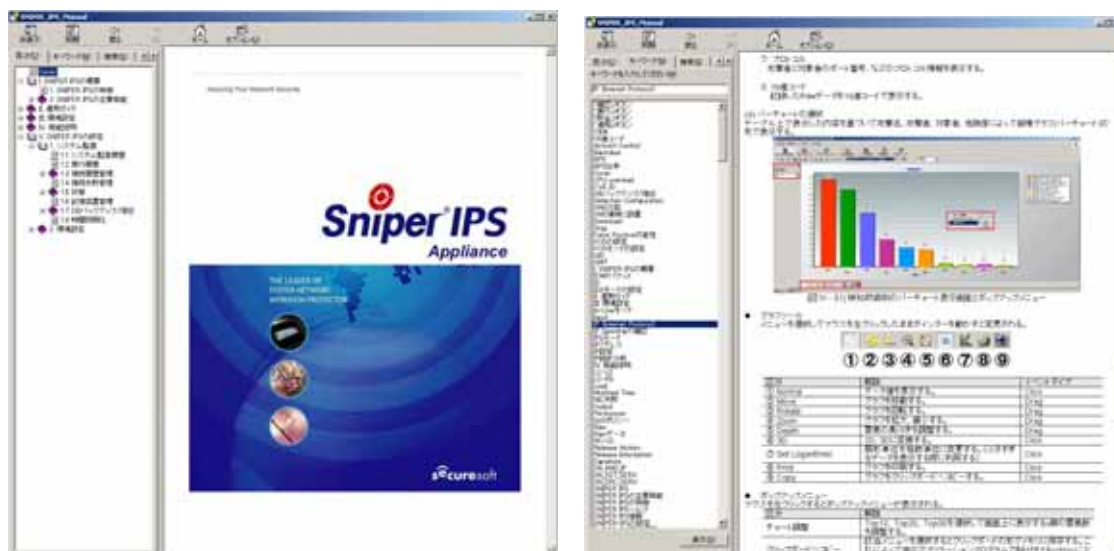
システム監査ではシステムの全般的な情報を管理します。システムの起動、接続管理、時間同期化(サーバとクライアントの時間を合わせる)、保存したデータをバックアップ、バックアップしたデータを復旧することなどができます。

3.6 環境設定

SNIPER-IPS の全体にかけてシステムの設定を管理します。ログの管理、ユーザ管理、ライブアップデート、ネットワーク、検知ポリシーなどを設定します。特に検知ポリシーでは登録されている攻撃(シグネチャ)に対して検知、防御、認定する攻撃回数、攻撃回数などをユーザがチューニングすることができます。

3.7 SNIPER ヘルプ

SNIPER-IPS のマニュアルが Windows のヘルプとして確認することができます。



4. SNIPER IPS の仕様

4.1 ラインナップ

| 区分 | A1000 | A2000 | A4000 | 備考 |
|---------------------------------|------------------------------|----------------------------------|------------------------------|-----------------|
| System | | | | |
| CPU | Intel Xeon Quad Core 1.6 x 1 | Intel Xeon Dual Core 2.0 x 2 | Intel Xeon Dual Core 3.0 x 2 | |
| Memory | 2GB | 4GB | 4GB | |
| DOM | 1GB | 1GB | 1GB | |
| HDD | 250GB(SATA) | 250GB(SATA) | 250GB(SATA) x 2 | |
| OS | Embedded OS | Embedded OS | Embedded OS | |
| Interface | | | | |
| Monitoring Interface | 1 x 10/100 | 1 x 10/100/1000 or 1 x Fiber(SX) | 1 x Fiber(SX) | 1 追加 最大 2Seg |
| Management Interface | 1 x 10/100/1000 | 1 x 10/100/1000 | 1 x 10/100/1000 | |
| | 1 x Serial(RJ45) | 1 x Serial(RJ45) | 1 x Serial(RJ45) | |
| HA Interface | 1 x 10/100/1000 | 1 x 10/100/1000 | 1 x 10/100/1000 | |
| Network Control | | | | |
| 2 Bypass | | | | |
| TAP(IDS Mode) | | 3Fiber(SX)のみ | | |
| HA | Fail-Open | | | |
| | Fail-Close | x | x | |
| | 手動制御 | x | x | |
| Etc. | | | | |
| Redundant Power | | | (2+1) | |
| Lockable Front Bezel | | | x | |
| Dimensions (mmW x mmD x mmH) | 430 x 427.2 x 88 | 430 x 427.2 x 88 | 432 x 431 x 134 | |
| Rack Type | 2U | 2U | 3U | |
| 重さ | 14.5Kg | 14.5Kg | 18.95Kg | |
| 電圧 | 100/240V 47/63Hz | 100/240V 47/63Hz | 90/264V 47/63Hz | |
| 消費電力 | 460W | 460W | 650W | |
| 動作温度 | 5C to 35C | 5C to 35C | 0C to 40C | |
| 保管温度 | -20C to 70C | -20C to 70C | -20C to 70C | |

1 2 セグメントをモニタリングする場合は性能が 15%ほど落ちる恐れがあります。

2 Bypass 機能は全ての機種で標準実装されています。(別途のデバイスではない)

3 A2000 の Copper タイプの場合は TAP (Mirroring) 機能を利用することができません。

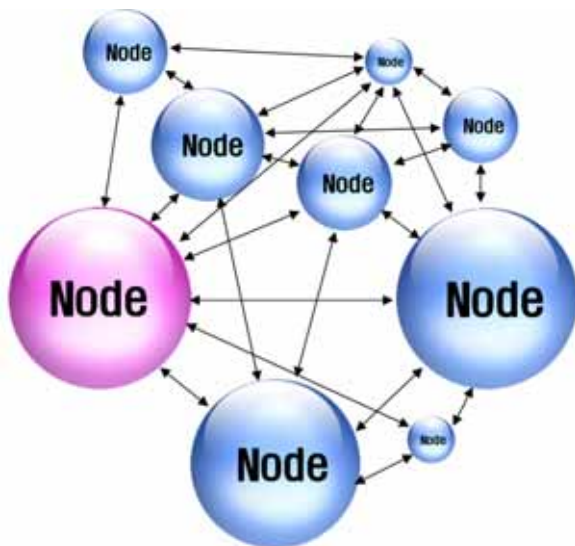
上記の情報は 2008 年 2 月から反映されるハードウェア仕様です。

4.2 多様な攻撃に対応

Winny 検知について

Winny とは

日本で開発されたファイル交換ソフトの一つで、高い匿名性と、独自の P2P 型匿名掲示板システムが特徴です。

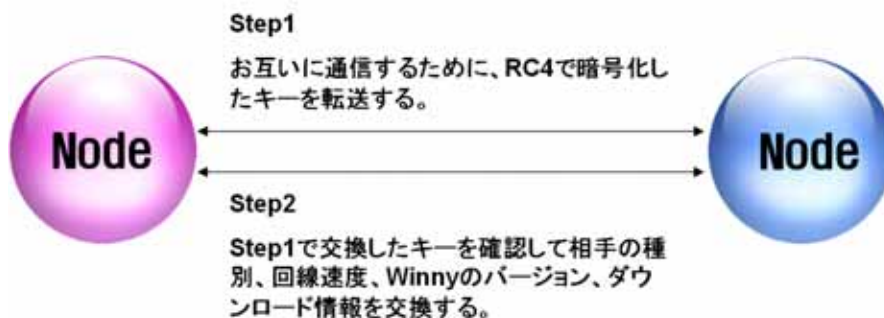


Winny ではノード情報を共有して接続しているノードへアクセスし相手の情報を取得することができます。

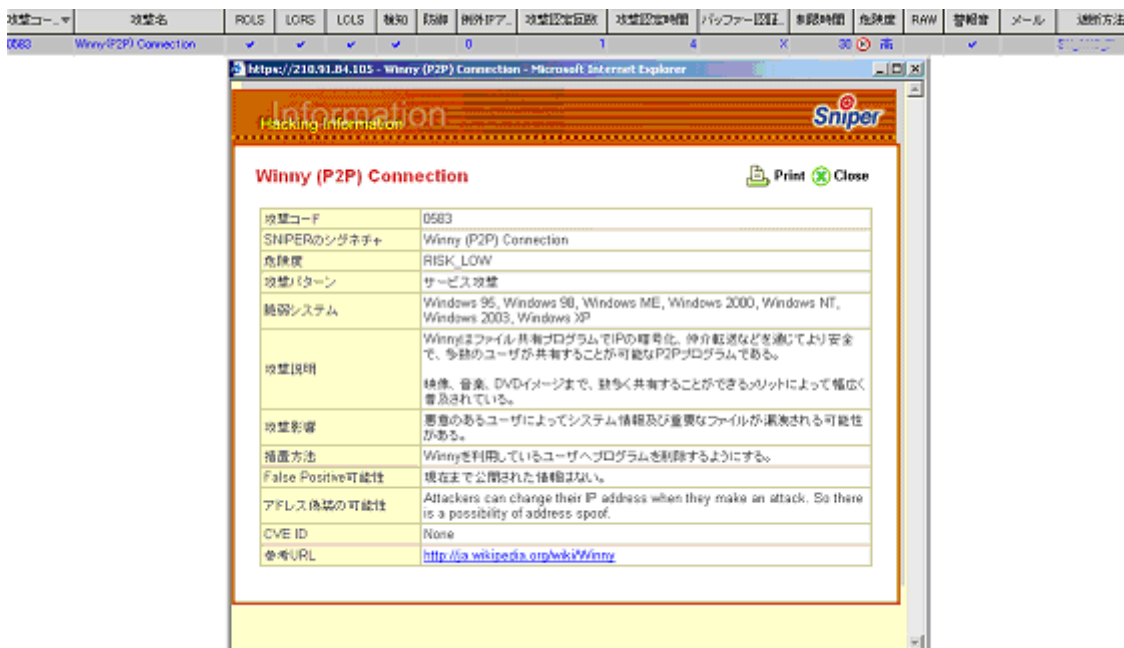
Winny は中央サーバを持たない純粋型の P2P ソフトで、所持ファイルのリストなどの情報は利用者間をバケツリレー式に転送されます。

今回のリリースから Winny を利用するネットワーク通信を検知・防御することが可能になりますが SNIPER IPS A2000 のモデルから対応します。ご注意ください。(A1000 は対応しません。)

検知方法



Winny の通信は上記のように最初からノード情報を確認しますが SNIPER IPS では暗号化されたパケットを複合化し、Step1 と Step2 のパケットを分析して Winny のバージョン情報を確認し、検知・防御することができます。

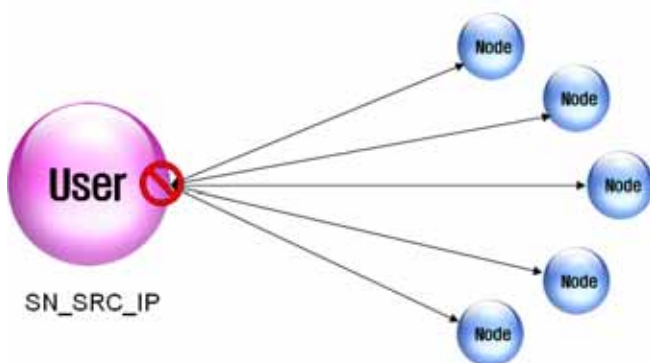


今回のリリースでは[環境設定] [検知ポリシー] [サービス攻撃]のカテゴリの中に Winnie 検知が可能なシグネチャとして登録されています。

| 攻撃名 | 攻撃元 | 攻撃対象 | 状態 | 危険度 | 検知日時 | Data Size | 状態 | 検知日時 | 検出 | 攻撃者情報 |
|-------------------------|-----------------|----------------|----|-----|------|-----------|----|----------------|-------|------------|
| Winnie (P2P) Connection | 10.10.30.2000 | 20146180030 | 検出 | 低 | | 0KB | 検出 | 06/25 15:19:30 | 00000 | TEST2 TEST |
| Frag Flooding | 10.10.30.120000 | 10.10.10.25483 | 終了 | 高 | 検出 | 400K | 検出 | 06/25 15:19:30 | 00000 | TEST2 TEST |

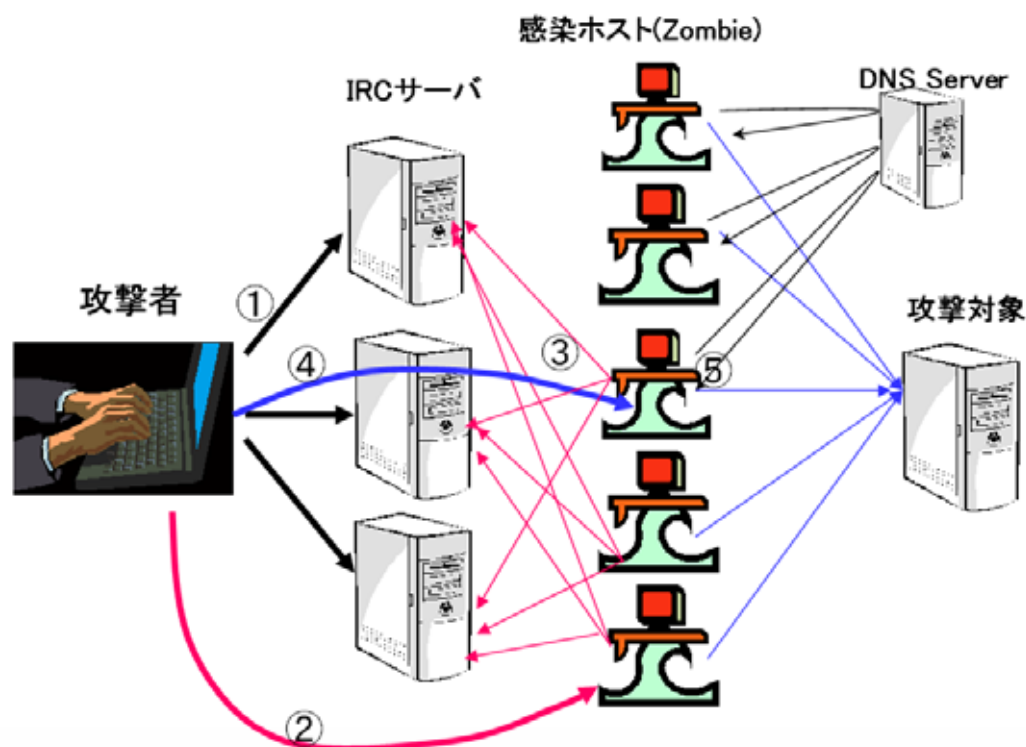
防御方法

SNIPER IPS では Winnie 通信を検知するに成功したら下記のように防御します。



Winnie を使用するユーザの IP をブロッキング(SN_SRC_IP 1:N)します。
 Winnie は多数のノードへアクセスするため、1:1 関係にして検知したら数多い検知イベントが発生してしまい、検知効率がよくありません。これを避けるために SNIPER IPS では Winnie を利用するユーザのみブロッキングするだけで一つのイベントで管理できます。

SNIPER IPS で防御設定したら Winnie を使用しているユーザの PC はインターネットへ接続することができなくなります。Winnie の使用を中止してある程度の時間が過ぎるとインターネット通信は可能になります。



- IRCBot : IRC の機能を利用してコントロールするシステム(PC)
- BoTNet : Bot に感染された PC, IRC Server など構成されたネットワーク

プライベート IRC チャンネルの open
 Bot 感染(ハッキング/Worm)
 IRC サーバへアクセスし、コマンドの待機
 リモートコントロールの実行
 DDoS 攻撃/違法行為

SNIPER IPS では BoT 攻撃に対応するために 1 次エンジンと 2 次エンジンに分けて対応しています。SNIPER IPS の 1 次エンジンで(パターンプロック/WEB CGI)は下記のように対応します。

- Bot に感染するとき
- Bot で利用されるサーバへアクセスするとき
- 攻撃者によるリモートでコントロールするとき

SNIPER IPS の 2 次エンジンで(サービス攻撃)は Bot が最終的に行うハッキングや DDoS 攻撃に対応します。複雑な Bot 攻撃行為を記憶しつつ、定められた条件を満たしたときに検知します。

4.3 シグネチャリスト(2700 個、2008 年 1 月現在)

シグネチャの数より如何にして攻撃を正確に検知・防御することが最も重要です。SNIPER-IPS では下記のように攻撃を分類して管理者が設定しやすくしています。

#1 サービス拒否

攻撃者が偽造・変造したパケットを送って対象サーバが正常なサービスが出来ないようにする攻撃手法です。ネットワークトラフィックを殺到したり、システム資源(CPU、メモリ等)に負荷をかけたりにしてシステムの性能を低下させることが特徴です。

[SecureSoft SNIPER IPS Signature]

FTP PASV DOS, ICMP Check Sum Error, ICMP Dos Echo, ICMP Ping of Death, ICMP Smurf, IGMP Nuke(KOD), IP Check Sum Error, OpenTear, Ping Sweep, Router Dos Attack, Snork Attack, TCP Check Sum Error, TCP Connect DOS, Telnet Flooding, UDP Check Sum Error, UDP Port Loopback, SYN Flooding, Land Attack, Mail Bomb, Mail Spam, Ping Flooding, UDP Flooding, ICMPUnreachable Storm, Windows Nuke, ...

#2 情報収集

攻撃者が特定のサーバやシステムを攻撃する前に対象サーバの脆弱性、ネットワークパス、ファイアウォールの有無等の情報を調べる攻撃手法です。

[SecureSoft SNIPER IPS Signature]

ACK Port Scan (F/W Scan), DNS BIND version request, DNS get host info, Finger, FIN Port Scan, FingerPrint, NULL Port Scan, FTP Login Brute FORCE, Host Sweep, HTTP Login Brute Force, POP3 Login Brute Force, Rlogin Login Brute Force, RPC Port Map Dump, RPC Port Map GetPort, SMB Login Brute Force, SYN Port Scan, Telnet Login Brute Force, TraceRoute, UDP Port Scan, XMAS Port Scan, ...

#3 プロトコル脆弱性

TCP/IP プロトコル規約上の問題点を悪用してネットワーク及びシステムに過負荷を発生させたり、サーバをダウンしたりして正常なサービスが出来ないようにする攻撃手法です。

[SecureSoft SNIPER IPS Signature]

ACK Strom, Corrupt IP Option, Hijacking, ICMP TearDrop, IGMP TearDrop, IP Spoofing, Source Routing, TCP TearDrop, UDP TearDrop, UDP Truncated Header, ...

#4 サービス攻撃

ソフトウェア変数管理上の問題であるオーバー・フローのバグ及び各種サービスの脆弱性を利用してサーバにアクセスしてコマンドを実行したり権限を獲得したりする攻撃手法です。

[SecureSoft SNIPER IPS Signature]

CDE dtspcd Overflow, CheckPoint RDP Attack, DNS Bind Overflow(Lion Worm), DNS name Overflow, DNS zone transfer, FTP Anonymous, FTP BackDoor, FTP Check User, FTP Command Line Overflow, FTP CWD ~root, FTP Login Fail, FTP Other Server, FTP PASV Crash, FTP Port Bounce, FTP site exec, HTTPD Overflow, LPD Attack, Mail Bad Command, Mail Bounce, Mail Command Overflow, Mail Debug, Mail Files, Mail Mailing List, Mail Programs, Mail Verify User, NETBIOS Datagram Service, NETBIOS Name Service, NETBIOS Session Service, NSI Rwhoisd Overflow, NTP Buffer Overflow, Password Overflow, Rlogin Buffer Overflow, Rlogin Login Fail, RPC amd Overflow, RPC autofsd Oveflow, RPC Bad Command, RPC bootparam, RPC cmsd Overflow, RPC mountd Overflow, RPC nfsd Overflow, RPC nisd Overflow, RPC pcnfsd Overflow, RPC Port Map Set, RPC Port Map Unset, RPC rexd Overflow, RPC ruers, RPC sadmind Overflow, RPC snmpXdmid Overflow, RPC statd Overflow, RPC status Overflow, RPC ttdbserver Overflow, RPC ypbind Overflow, RPC yppasswd Overflow, RPC ypserv Overflow, RPC ypupdated Overflow, SNMP Overflow, Telnet Login Fail, Telnetd Overflew, User ID Overflow, ...

#5 WEB CGI

ウェブ上の CGI のバグを利用してコマンドを実行したり権限を獲得したりする攻撃手法です。

[SecureSoft SNIPER IPS Signature]

CGI AnyForm, CGI guestbook.cgi, Count.cgi overflow, CGI campas, CGI aglimpse, CGI faxsurvey, CGI htmscript, CGI info2www, CGI npb-test-cgi, CGI pfdisplay.cgi, CGI php, CGI webdist.cgi, CGI win-c-sample.exe, CGI convert.bas, "::DATA" append, winnt/win.ini, /iissamples/aexp3.htr, /scripts/wsis.dll/Wservice=anything?, .htaccess, .htpasswd, /....., ./access, /.bash_histroy, /.html, /.jsp/WEB-NIF/classes/Env.java, /.passwd, /....., /?.jsp, /?PageServices, /?wp-cs-dump, /?wp-html-rend, /_AuthChangeUrl, /_private, /_vti_adm/admin.dll, /_vti_bin/vti_aut/author.dll, /_vti_bin/fpcount.exe, /_vti_log, /-guest, /blabla, ida, /blabla.idc, /blabla.idq, /blabla.idw, /boot.ini, /cgi-bin/bash, /cgi-bin/changepw.exe, ...

#6 Backdoor

悪意的な目的で対象システムにあるプログラムを設置して情報を獲得したり、システムをクラッシュしたりする攻撃手法です。

[SecureSoft SNIPER IPS Signature]

Acid Battery 1.0, Aims Spy, AOL Trojan 1.1, Attack FTP/Satans Backdoor, Back Orifice 2000, BigGluck/Tiny Telnet Server, GirlFriend, NetBus, Gatecrasher, DeepThroat, SubSeven, BackConstruction, BladeRunner, DeltaSource, DolyTrojan, Eclipse 2000, FileNail, FireHotcker, Hack Office Armageddon, Gjamer, HackersParadise, ICQ Killer, ICQTrojan, InCommand, Insane Network 4, Mini Command 1.2 Access, NetBusPro, NetSphere Final 1.31.337, NetSpyDK, Online Key logger, OOOLT, PC-Crasher, Portal of Doom, ...

#7 ユーザ定義

管理者はプロトコル、ポートなどの情報を入力して攻撃と登録することが可能です。

詳細な検知・防御条件

- 検知文字列(テキスト、バイナリー)
- OFFSET の指定
- ネットワーク領域の区分: *1RCLS, LCRS, LCLS
- 検知の例外メカニズム
- 攻撃回数/攻撃時間の調整
- 防御する時間の制限
- 攻撃方向の指定 (Request, Response)

*1 RCLS:RemoteClient-LocalServer, LCRS:LocalClient-RemoteServer, LCLS:LocalClient-LocalServer

#8 パターンブロック

パターンブロックはあるパケットに対してシグネチャとの比較する処理を行わず、すぐブロッキングすることができます。致命的なワームである DoS、DDoS または DRDoS のような攻撃 (MyDoom など) を登録しておくことによって素早くブロッキングすることができます。