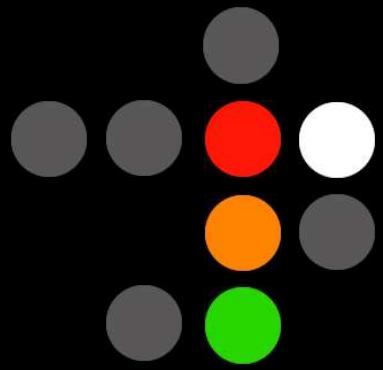
Protecting against DoS Attacks



radware

Glen Salomon

Regional Account Manager

The need for DoS Protection

DDoS Attacks

DDoS attacks were the second-most expensive cyber crime in ’03/’04
(CSI/FBI 2004 Computer Crime & Security Survey)

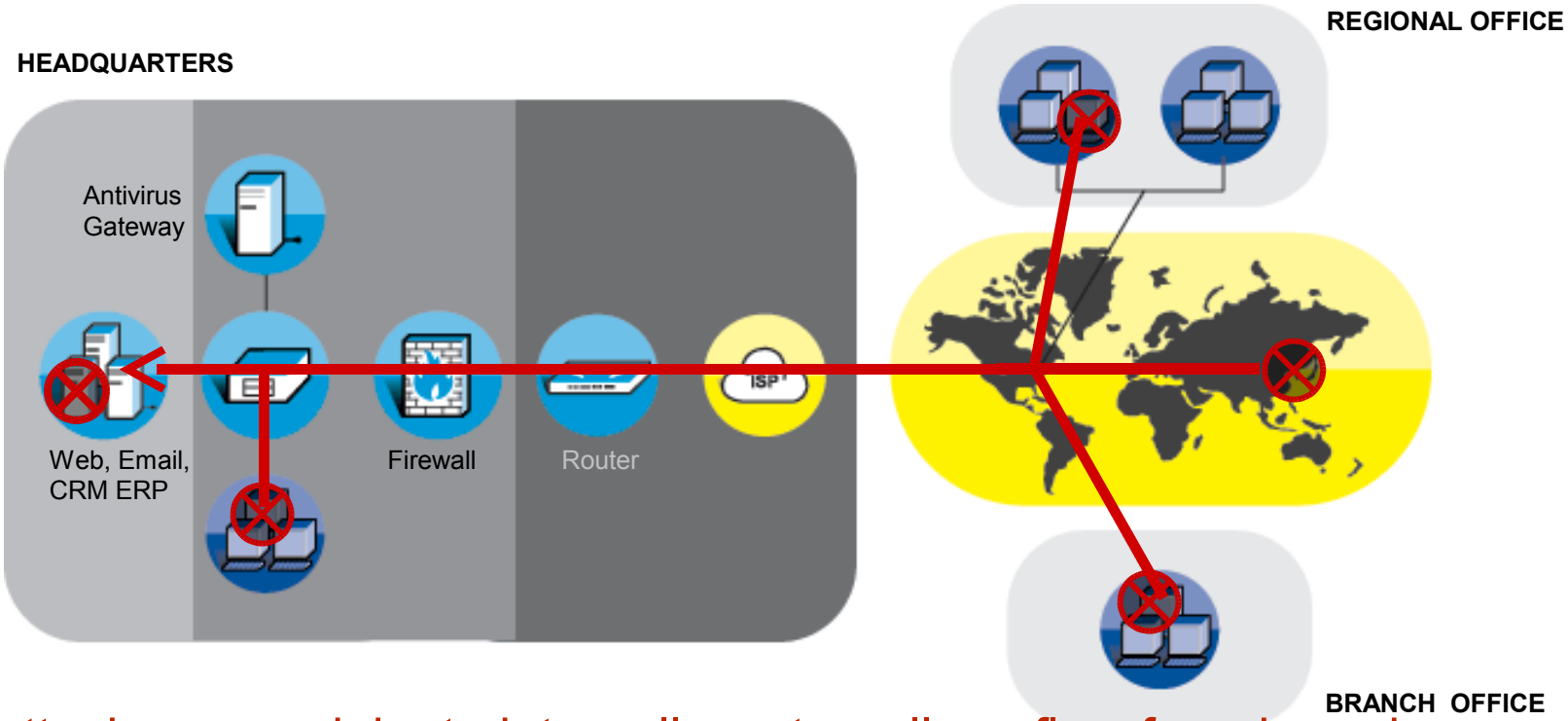
Attackers are using viruses and worms to install BOT (distributed-DOS relay kits) on compromised machines

- For example Code Red, MydoomA and Mydoom B worm variants

Massive distributed DOS attack are generated using several thousand remotely controlled "bots" machines

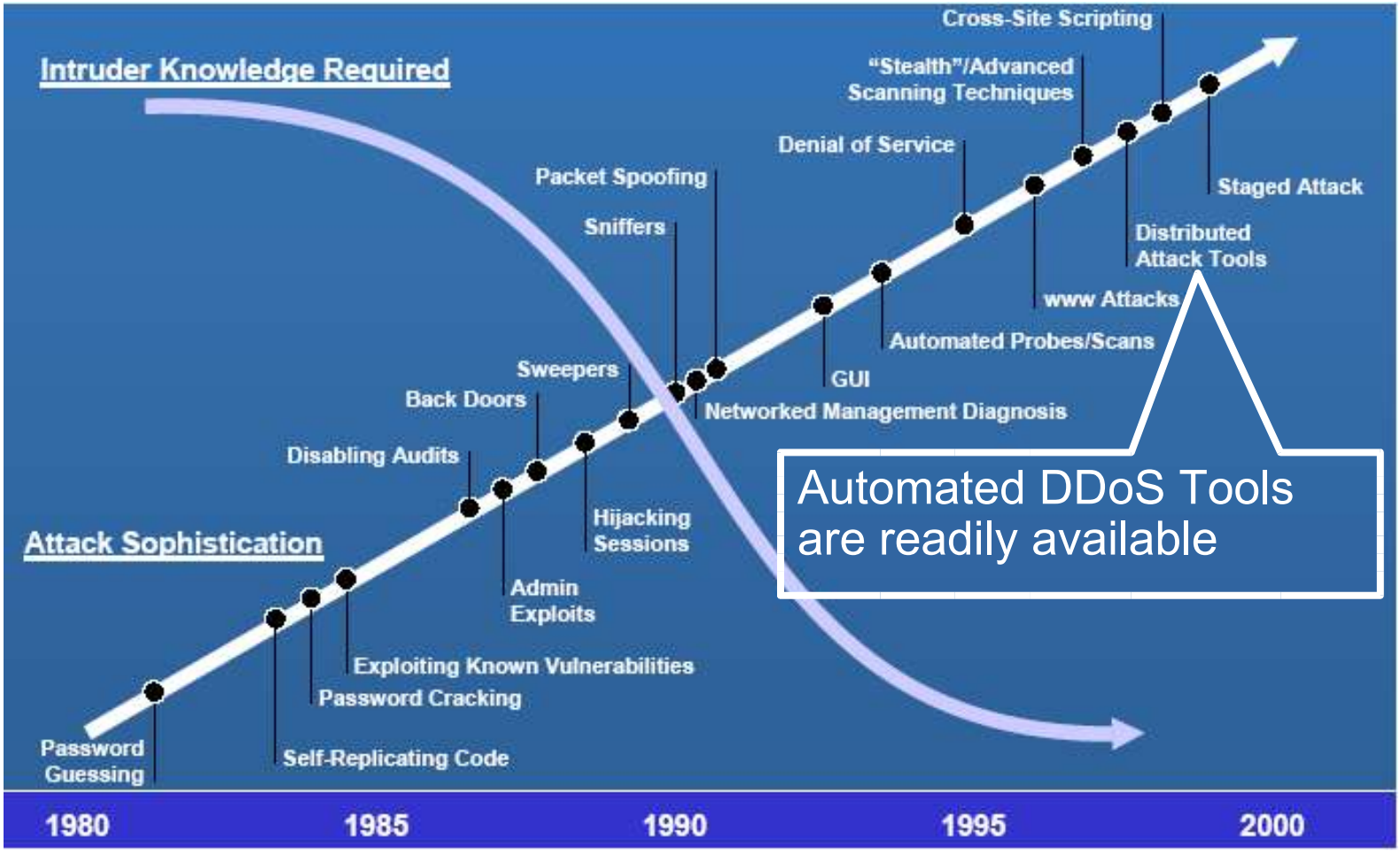
DoS attack tools are widely available

End-To-End Security Challenges

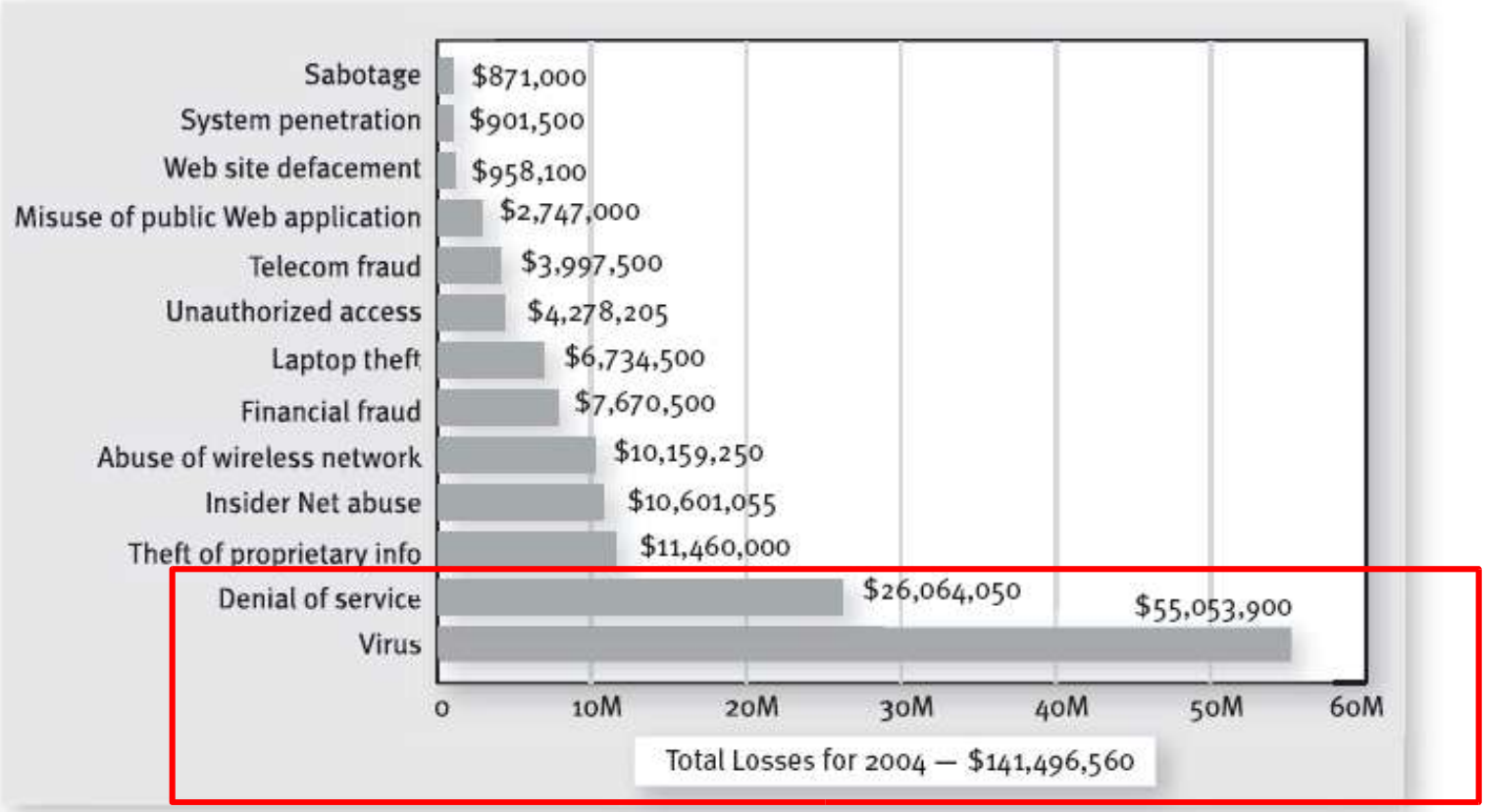


- DoS attacks may originate internally, externally or flow from branches
- Application availability is at risk from application level attacks such as worms, viruses and DoS

Why Attacks Are Increasing



Cost of Security Violations



CSI/FBI 2004 Computer Crime and Security Survey
Source: Computer Security Institute

2004: 269 Respondents

Average annual DoS cost : **$100,000**

Who are the victims?

eWEEK ENTERPRISE NEWS & REVIEWS — ZIFF DAVIS INTERNET

REVIEWS · OPINIONS · CASE STUDIES · TOPICS · INDUSTRIES · TOOLS · WHITE PAPERS

SEARCH eWEEK

SUBSCRIBE TO eWEEK — My Account | Sign In Not a member? Join now

Home > Topics > Security > News > **Spyware Critic Knocked Offline by DDoS Attack**

Security

Spyware Critic Knocked Offline by DDoS Attack

By Ryan Naraine

February 9, 2005

TALKBACK Comment on this article

Be the first to comment on this article

Harvard researcher Ben Edelman, one of the most vocal critics of spyware purveyors, fell victim to a massive DDoS (distributed denial-of-service) attack over the past 24 hours.

Edelman's **Web site,** which publishes detailed research reports on spyware, was knocked offline for much of Monday and Tuesday by a DDoS attack that crippled the server capacity.

RELATED LINKS

- DDoS Attack Knocks Out DoubleClick Ads
- Akamai DDoS Attack Whacks Web Traffic, Sites
- DDoS Attacks for the Common Man
- Fake Microsoft Mail Is Spyware Phishing Attack
- Anti-Spyware Consortium Falls Apart

POLITICS

China promises to work on N Korea

said it is working to trace the source of the

Vote

Dos Attacks Hidden Victims

The press focuses on the target of DDoS attacks as the victim

In reality there are many victims in a DDoS attacks:

- The final target (web site)
- The systems controlled by the intruder
- Enterprise networks of infected systems
- Enterprise & Carriers mail servers
- Carrier's backbone

What is needed

There is a need for a DDoS mitigation system that will provide the following:

Protect potential targets from incoming DDoS attacks

Protect Enterprise network's PCs from propagation of worms that contain DDoS BOT codes

Protect Enterprise network's bandwidth from being consumed by outbreak of outbound DDoS traffic

Protect Enterprise & Carrier Mail servers

Protect Carrier's backbone from incoming and outgoing DDos Attacks

What is needed (part 2)

Preventive measure:

Identify & block propagation of worms that contain DDoS BOT codes

Mitigating DDoS outbreak:

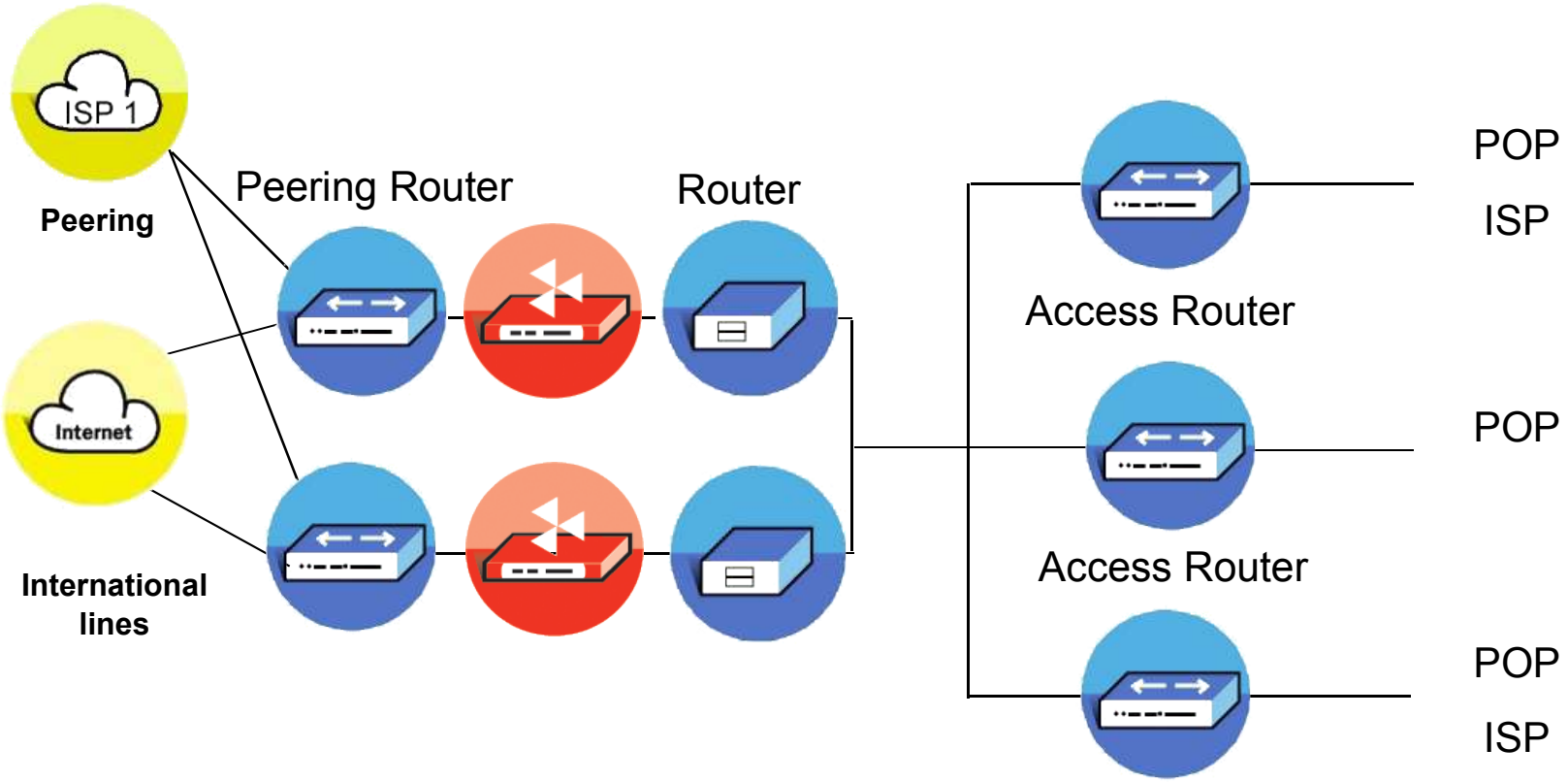
Identify & block incoming DDoS attacks

Identify & block outgoing DDoS attacks

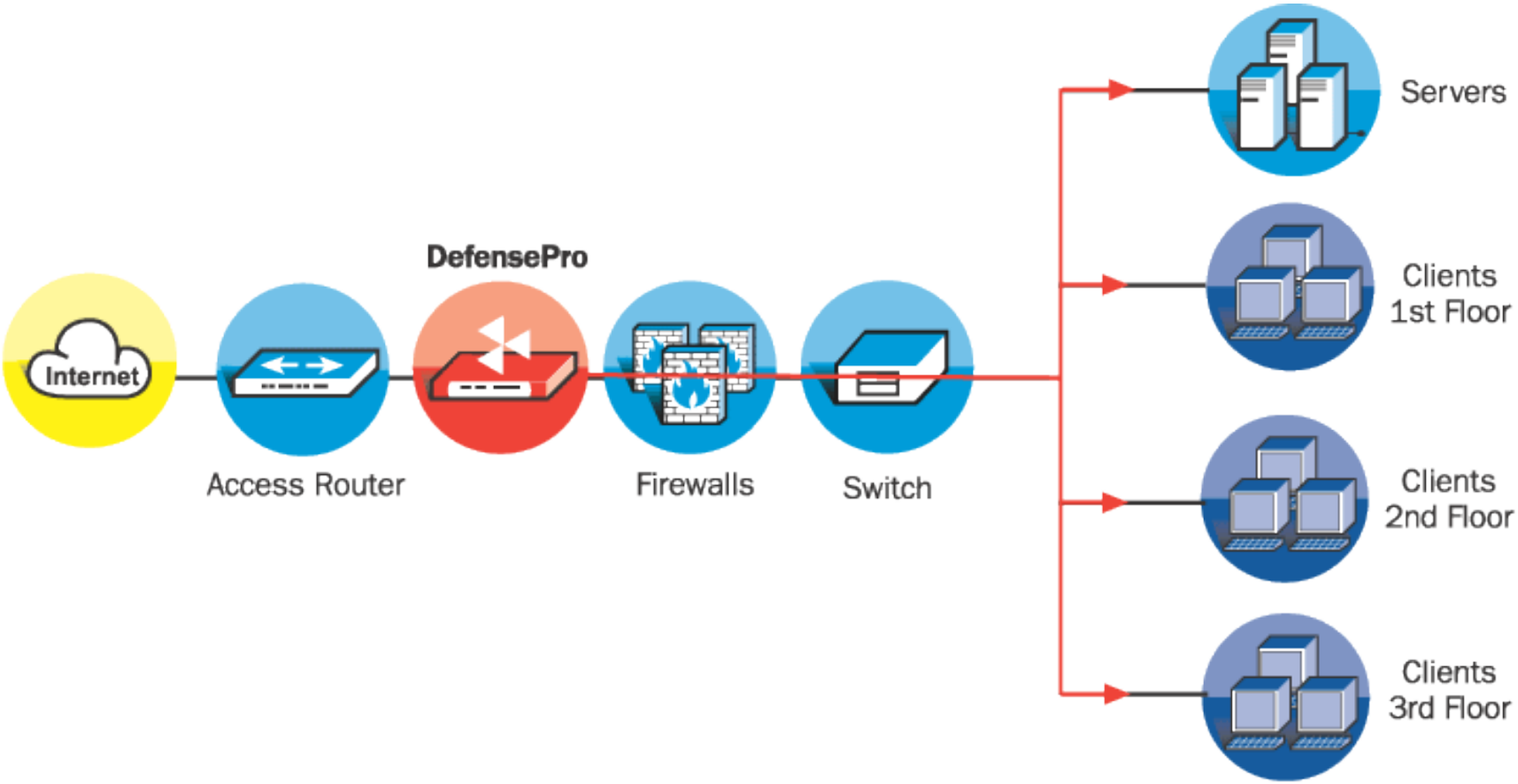
Ensure the continuous operation of mission critical application even during incoming/ outgoing DDoS attacks

Carrier network security – Central POP

Cleaning the Carrier network



Inline 3-Gbps Security Switching



Introducing Radware

We are a **Application Infrastructure** vendor

We provide enterprises with
availability, **performance** & **security**
for their **mission critical applications**

We offer it **end-to-end:**
From the **headquarters** to the **branch** office

Who we are

Founded in ’97, Public company since Sept. ‘99 (NASDAQ: RDWR)

Selling in over 40 countries, more than 130 resellers & distributors world wide

$68M Total sales for 2004 & **profitable**

25% annual growth over 2003, exceeded expectations over the last 15 quarters

$165M in cash, **No debt**

Leading Customers

Over 3000 customers across industrial sectors

* Sample List

COMVERSE | SONY | AccuWeather.com | Continental Airlines

HSBC | TOSHIBA | ebay The World's Online Marketplace™ | SAKS FIFTH AVENUE

上海證券交易所 SHANGHAI STOCK EXCHANGE | 中国电信 CHINA TELECOM | TOYOTA | ADP

citibank | FannieMae | verizon | cingular WIRELESS

Industry Award Recognition

Radware's Roster of Awards stands as testament to our continued technology innovation & leadership

US Patents:

1. **Triangle redirection** (Issued June 19, 2001)
2. Multiple link management in **LinkProof** (Issued December 16, 2003)
3. **Network Proximity** (Issued April 6, 2004)

* Sample List

2002 | 2003 | 2004 | 2005

Analysts Recognize Radware

Gartner Places Radware in the **Leader Quadrant** in Web-enabled Application Delivery Magic Quadrant

IDC: **Second** largest market share by port shipment (17.1%)

Gartner Places Radware in the **Challenger** Quadrant in enterprise security Magic Quadrant

Introducing Radware DefensePro

3-Gbps DoS Protection

DefensePro delivers multi-Gigabit DoS protection, attack isolation and bandwidth management. Identifying traffic anomalies in real-time, DefensePro prevents DoS/DDoS and SYN floods, safeguarding against all illicit traffic patterns.

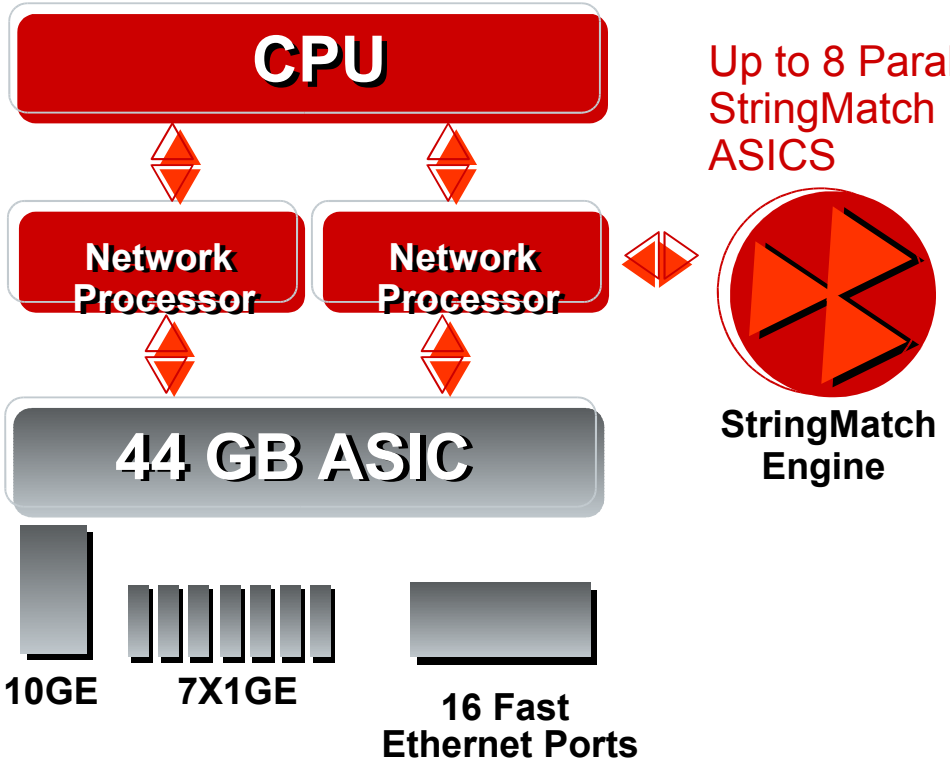
3Gbps Security Switch Architecture

4-Tier **Security Switching Architecture** & **String Match Engine** for **1000 X accelerated pattern** and policy matching

Session Management

3 Gbps Forwarding Blocking & SYN Cookies

Wire Speed Data Transfer & Connectivity



Up to 8 Parallel StringMatch ASICS

Isolate, Block & Prevent DoS Attacks

Mutli-Gigabit inline security switching safeguard from Incoming & outgoing DoS attacks

High port density, up to 11 segments protection enables high capacity scanning across multiple network segments with a single device

Diversified DoS mitigation technologies secures customers against abnormal traffic patterns and server downtime

Attack isolation prevents DoS attack spread across servers, applications & users

Intrusion prevention, blocking DoS BOT worms

Traffic shaping ensuring service levels even when under DoS attack

Security Switch Architecture Benefits

Highest port density in industry, multiple segment scanning for immediate security ROI

Unmatched 1000X inspection acceleration with up to 256,000 **parallel pattern searches**

Minimal performance degradation with full database detection

Minimal latency with added signatures

3Gbps packet blocking

Gigabit forwarding of all secure traffic

Diversified DoS/SYN Protection Technologies

1) **Real time blocking of DDoS BOT worms**

2) **Bandwidth Management to shape traffic, block 'unknown' attacks** & manage infrastructure load capacities

3) **DoS Shield – protection from all known DoS / DDoS attacks**

4) **SYN Cookies Against ALL SYN Floods Blocking up to 700,000** SYN / sec while forwarding legitimate traffic

5) **DHCP Flood protection** – maintaining uninterrupted network access

Multi-gigabit Intrusion Prevention

Bi-directional scanning, stateful deep packet inspection **& Intrusion Prevention,** securing servers, applications & users against **over 1,700+ :attacks**

Viruses -

Worms -

Trojans -

Port-Scanning -

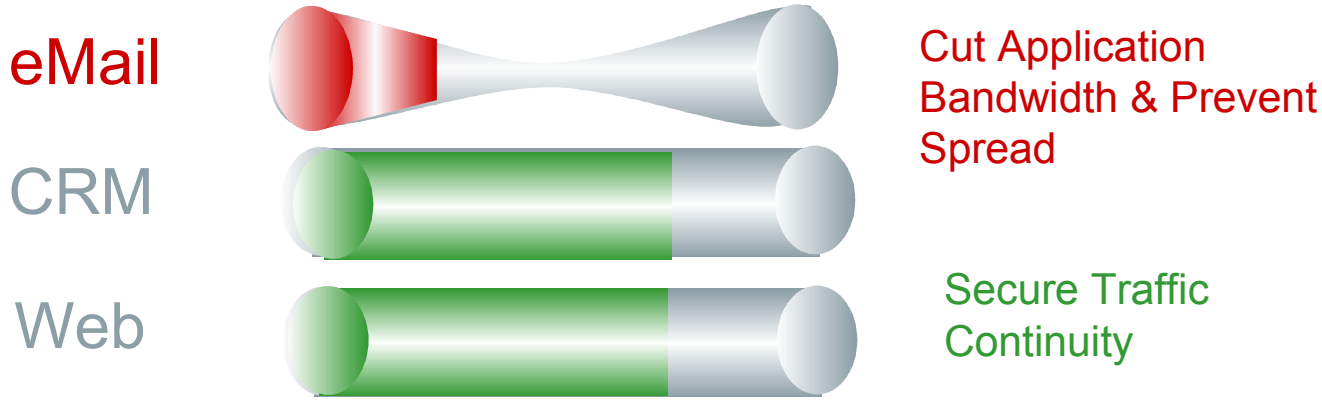
Protocol Anomalies -

Dynamic Traffic Shaping

"Adding more bandwidth may only improve the response of non-essential applications. It does not guarantee that the bandwidth will be available to the applications that need it most,"

"Traffic Management: Optimizing the Enterprise Network for Maximum Business Value," Yankee Group, October 03

- End-to-end bandwidth management & QoS to guarantee Service Level Agreements & accelerate application performance even when under attack

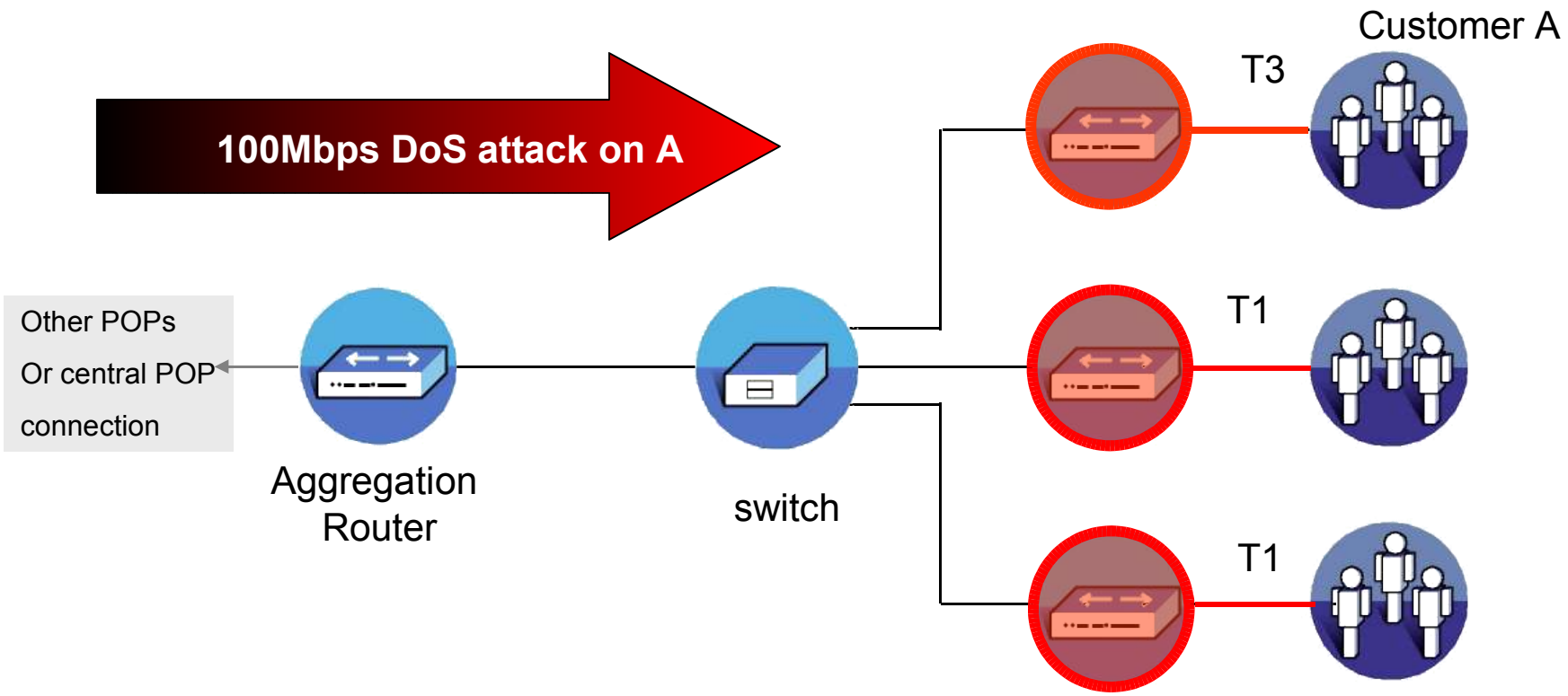


DoS Shield

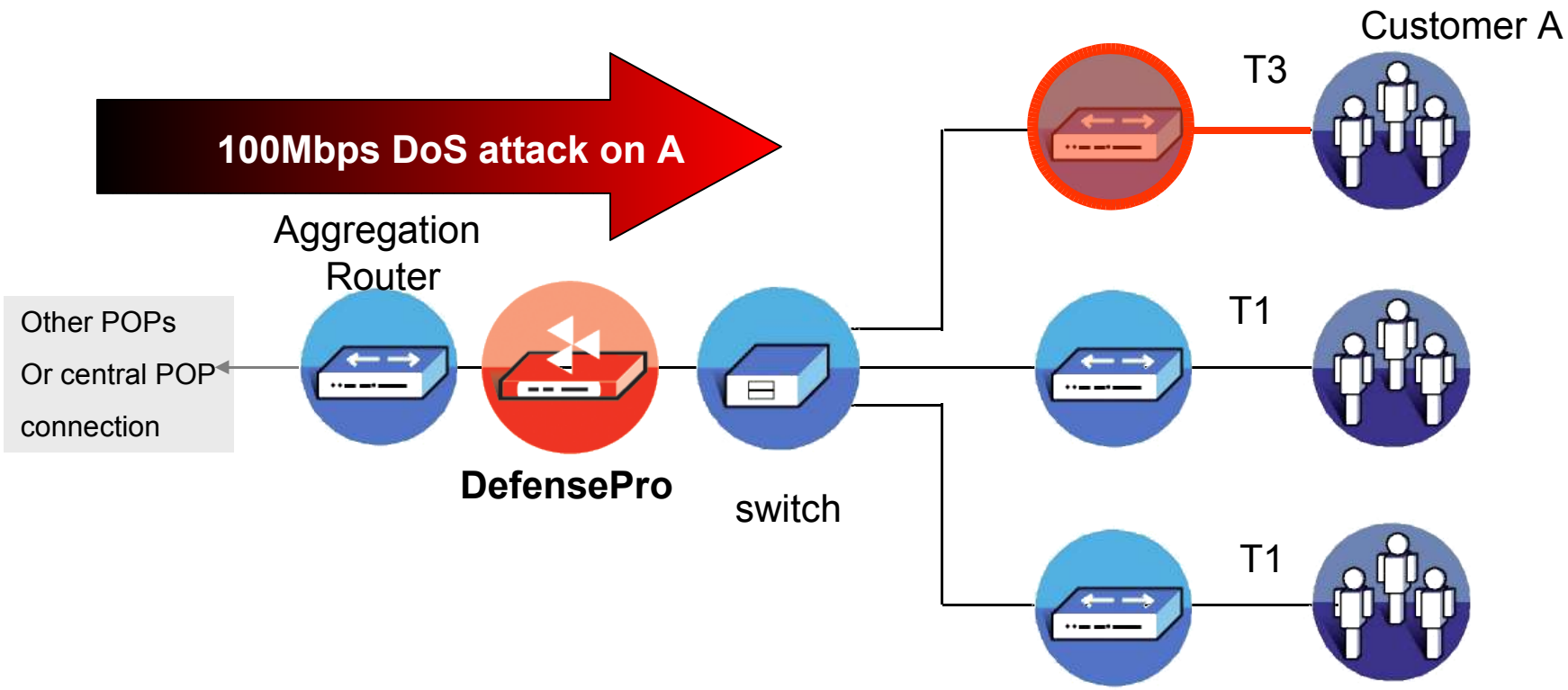
Signature based protection coupled with traffic anomalies detection mechanism

- Mitigate all automated DDoS attack tools available on the wild
- Advanced sampling mechanism guarantees effective mitigation even in high throughput environments

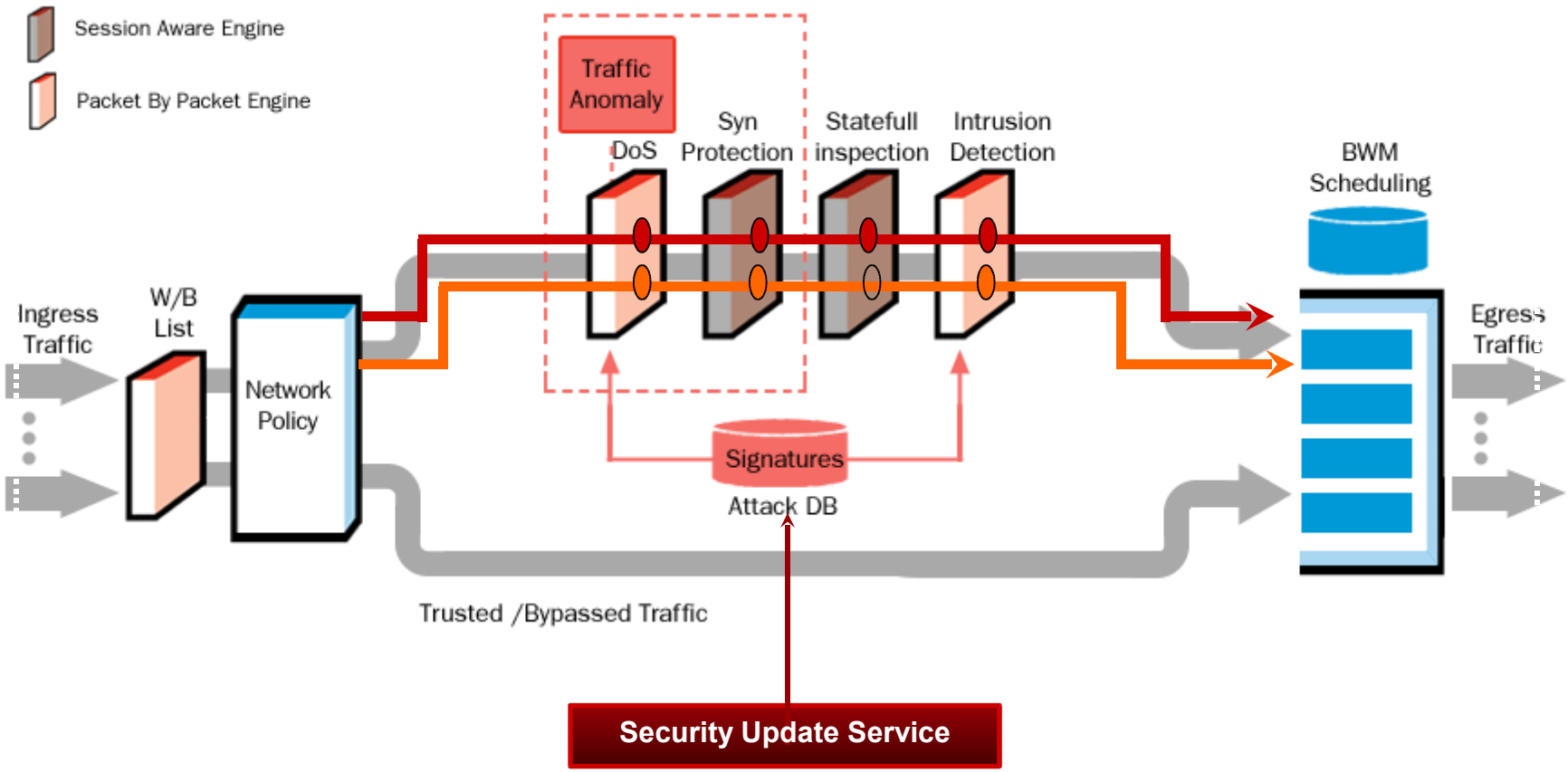
Attack Isolation in Action



Attack Isolation in Action



DefensePro architecture



DNS / DHCP protection

DNS server protection

- DoS Shield
- Signature Based (IPS)
  - Protect from common DNS exploits
- Behavioral Based Protection (BWM)
  - Limit # of user's DNS requests per second
- State Machine Awareness (Protocol Anomaly)
  - Protect from DNS replies received without prior query

DHCP Server protection

- DoS Shield
- Behavioral based protection
  - Limit # of user's DHCP requests per second

Securing VoIP is unique

- Voice is arguably any company's most mission-critical business application
  - No telephone usually means no business
- VoIP traffic is subject to DOS attacks that can introduce delays to the voice stream

Securing VoIP with DefensePro

DoS Mitigation Capabilities

- DoS Shield
- Syn Cookies
- Limit # of session per user (Bandwidth Management)

IPS capabilities

- Protect from OS vulnerabilities
- Protection from SIP exploits

Traffic Shaping

- Ensure VoIP sessions bandwidth even under attacks

DefensePro Product Family

DefensePro Product line

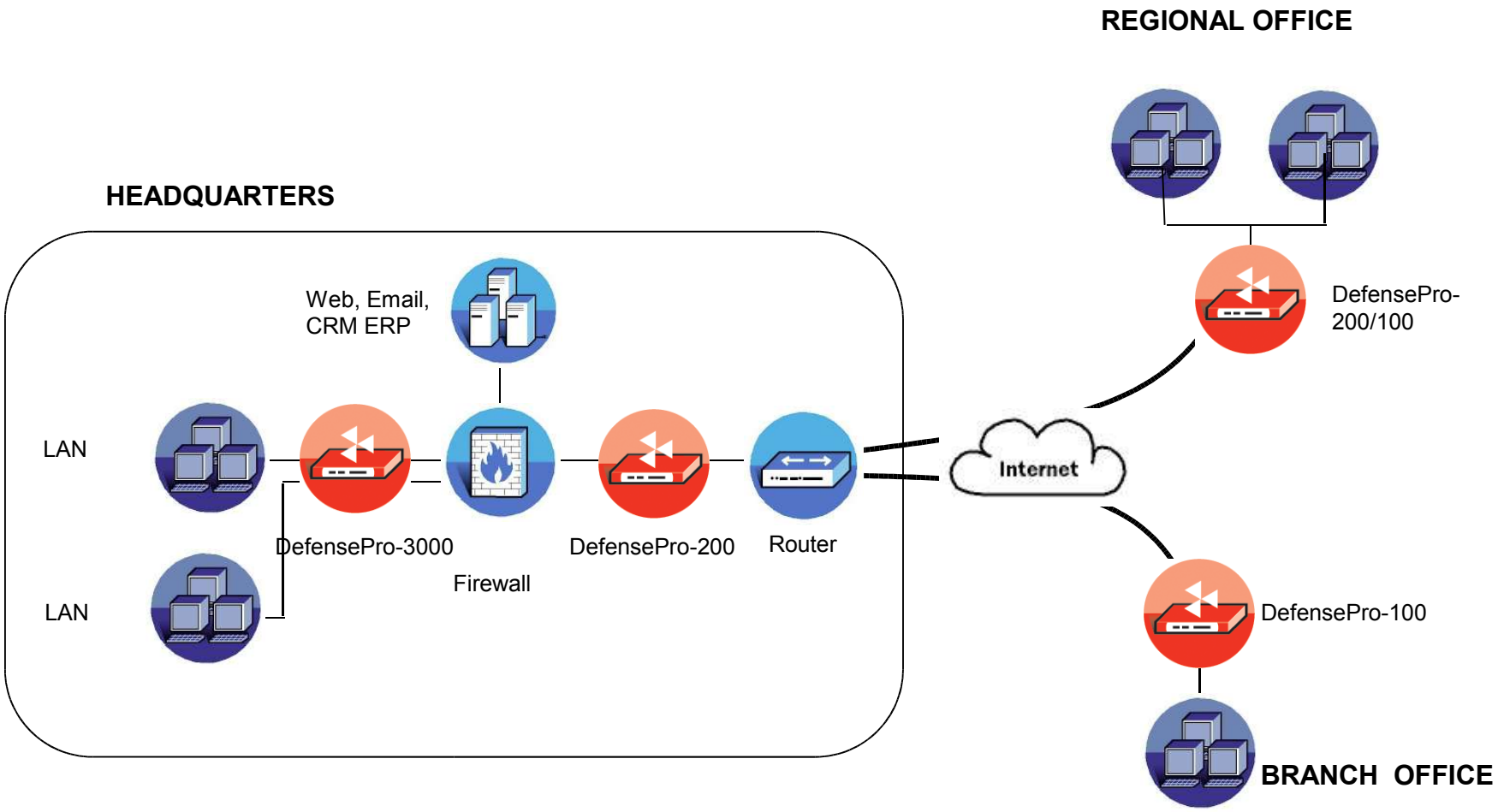
- DefensePro-3000
  - HQ / Core Network / Data Centers

- DefensePro 1000
  - HQ / Core Network / Data Centers

- DefensePro 200
  - Corporate GW

- DefensePro-100
  - Branch/ regional offices
  - CPE for MSSP

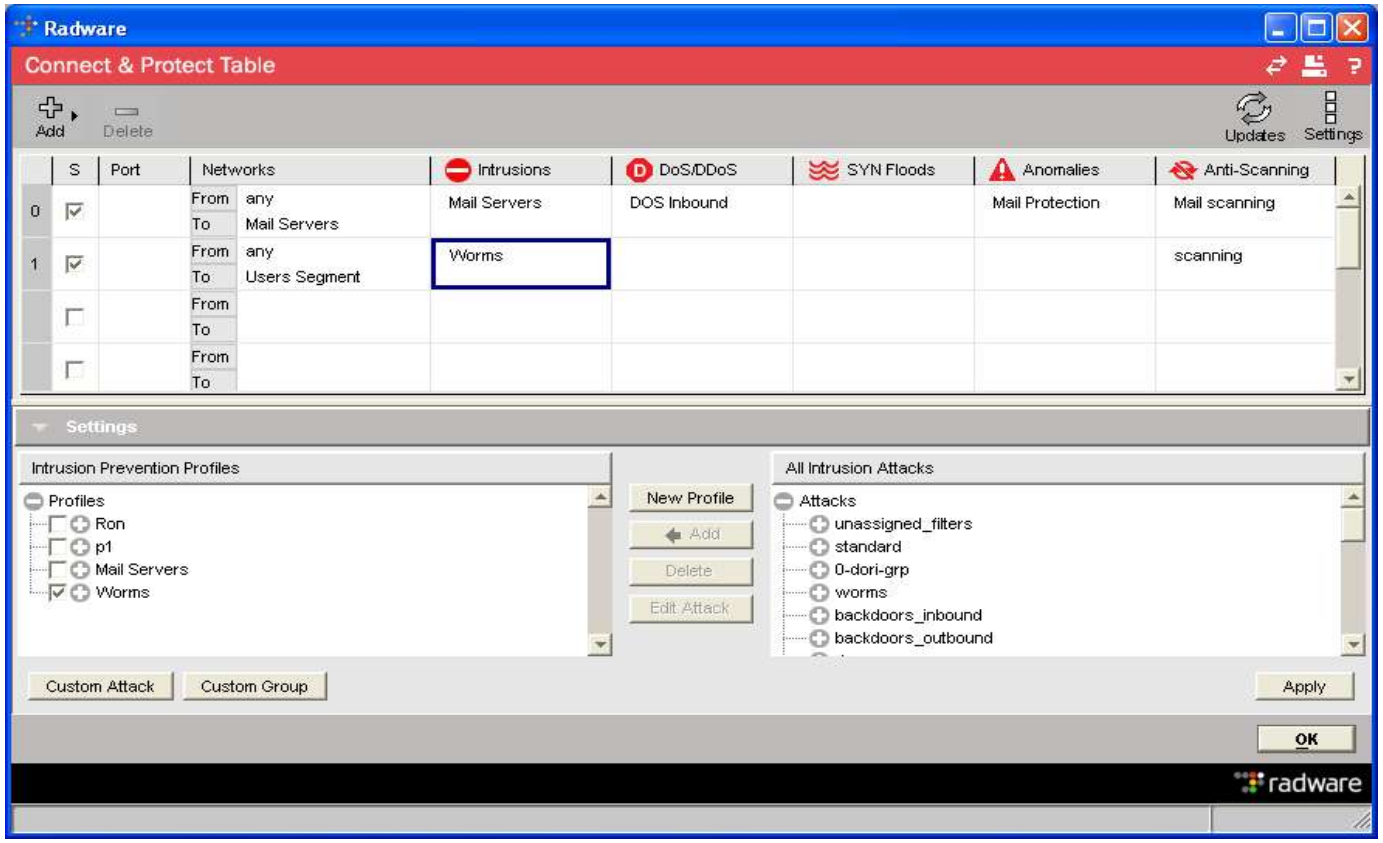
Product Positioning



DefensePro Management Application

Ease of use - 1st Time Wizard

Centralized Security Management



Connect & **Protect Set-up**: of ALL Security Attack Services
Intrusions, DoS, SYN Floods, Anomalies & Anti-Scanning

Configware Insite - C:/Documents and Settings/udi/ConfigwareInsite/UserFiles/Untitled.rdw

File Device SynApps General Statistics Help

Dashboard Logs Reports Map Split Delete Goto Filter Search TFTP Prefrences User Define Executive Export

Device 176.200.111.99 Period All Rows Per Page: 20 Jump to: Update

Report List

- Pre-define
  - Top Attacks
  - Top Attacks by Category
  - Top Attack Targets
  - Top Attack Sources
  - Top Attack Targets Bandw
  - Number of Attacks Over
  - Attacks By Severity
  - Intrusions
  - DoS
  - Anomalies
  - Anti-Scanning
  - SYN protection
- User
  - My Reports 1
  - My Reports 2

Activate Filter

- Filter#01
- Filter#02
- Filter#03

Top Attacks << Previous 1 2 3 4 Next >>

	Attack Time	Attack Name	Physical Port	Action	Category	Protocol	Source Address	Source
3	01/11/2004-18:00:55	Worm-NetSky-Q1	1	drop	Intrusions	TCP	194.90.9.4	NA
	01/11/2004-18:00:49	Worm-NetSky-Q2	1	drop	Intrusions	TCP	212.150.48.98	47081
	01/11/2004-18:00:19	Worm-Possible-pif-Worm	1	drop	Intrusions	TCP	61.66.170.96	4836
8	01/11/2004-17:59:49	Worm-NetSky-Q2	1	drop	Intrusions	TCP	NA	NA
	01/11/2004-17:59:24	Worm-Bagle-AV-2	1	drop	Intrusions	TCP	194.90.9.4	61096
	01/11/2004-17:59:19	Worm-Possible-pif-Worm	1	drop	Intrusions	TCP	61.66.170.96	4836
	01/11/2004-17:58:49	Worm-NetSky-Q2	1	drop	Intrusions	TCP	212.150.48.98	47081
	01/11/2004-17:58:29	Worm-Possible-pif-Worm	1	drop	Intrusions	TCP	61.66.170.96	4836
	01/11/2004-17:58:24	Worm-Bagle-AV-2	1	drop	Intrusions	TCP	194.90.9.4	61096
	01/11/2004-17:58:29	Worm-Possible-pif-Worm	1	drop	Intrusi			
	01/11/2004-17:58:29	Worm-Possible-pif-Worm	1	drop	Intrusi			

Provides Attack Description and Packet Data

Attack Description

Name: Worm-NetSky-Q2

Attack Description:
This alert indicates a Netsky-Q worm email attachment was detected.

Packet

Source	Destination	Protocol	Source Port	Destination Port	Length
10.204.180.2	212.88.149.241	ICMP	57638	20528	240

Configuration Statistics Security Reports

radware

Configware Insite - C:/Documents and Settings/udi/ConfigwareInsite/UserFiles/Untitled.rdw

File Device SynApps General Statistics Help

Dashboard Logs Reports Map Split Delete Goto Filter Search TFTP Prefrences: User Define Executive Export

Device 176.200.111.99 Period All Rows Per Page: 20 Jump to: Update

Report List

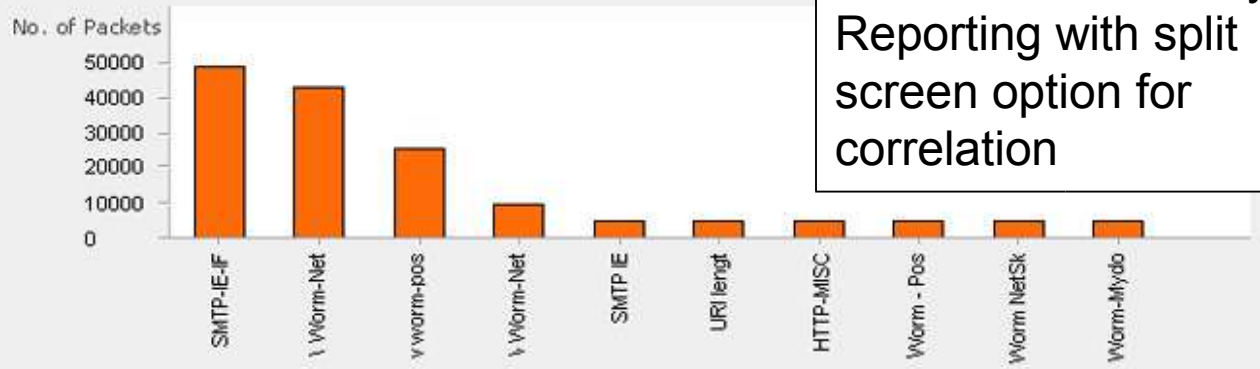
- Pre-define
  - Top Attacks
  - Top Attacks by Category
  - Top Attack Targets
  - Top Attack Sources
  - Top Attack Targets Bandw
  - Number of Attacks Over
  - Attacks By Severity
  - Intrusions
  - DoS
  - Anomalies
  - Anti-Scanning
  - SYN protection
- User
  - My Reports 1
  - My Reports 2

Activate Filter

- Filter#01
- Filter#02
- Filter#03

Top Attacks << Previous 1 2 3 4 Next >>

	Attack Time	Attack Name	Physical Port	Action	Category	Protocol	Source Address	Source
3	01/11/2004-18:00:55	Worm-NetSky-Q1	1	drop	Intrusions	TCP	194.90.9.4	NA
	01/11/2004-18:00:49	Worm-NetSky-Q2	1	drop	Intrusions	TCP	212.150.48.98	47081
	01/11/2004-18:00:19	Worm-Possible-pif-Worm	1	drop	Intrusions	TCP	61.66.170.96	4836
8	01/11/2004-17:59:49	Worm-NetSky-Q2	1	drop	Intrusions	TCP	NA	NA
	01/11/2004-17:59:24	Worm-Bagle-AV-2	1	drop	Intrusions	TCP	194.90.9.4	61096
	01/11/2004-17:59:19	Worm-Possible-pif-Worm	1	drop	Intrusions	TCP	61.66.170.96	4836
	01/11/2004-17:58:49	Worm-NetSky-Q2	1	drop	Intrusions	TCP	212.150.48.98	47081
	01/11/2004-17:58:29	Worm-Possible-pif-Worm	1	drop	Intrusions	TCP	61.66.170.96	4836
	01/11/2004-17:58:24	Worm-Bagle-AV-2	1	drop	Intrusions	TCP	194.90.9.4	61096
	01/11/2004-17:58:29	Worm-Possible-pif-Worm	1	drop	Intrusions	TCP	61.66.170.96	4836
	01/11/2004-17:58:29	Worm-Possible-pif-Worm	1	drop	Intrusions	TCP	61.66.170.96	4836



New unified Security Reporting with split screen option for correlation

Configuration Statistics Security Reports

radware

Configware Insite - C:/Documents and Settings/udi/ConfigwareInsite/UserFiles/Untitled.rdw

File Device SynApps General Statistics Help

Dashboard Logs Reports Map Split Delete Goto Filter Search TFTP Prefrences User Define Executive Export

Device 176.200.111.99 Period All Rows Per Page: 20 Jump to: Update

Report List

- Pre-define
  - Top Attacks
  - Top Attacks by
  - Top Attack Targ
  - Top Attack Sour
  - Top Attack Targ
  - Number of Attac
  - Attacks By Sev
  - Intrusions
  - DoS
  - Anomalies
  - Anti-Scanning
  - SYN protection
- User
  - My Reports 1
  - My Reports 2

Activate Filter

- Filter#01
- Filter#02
- Filter#03

Top Attacks

<< Previous 1 2 3 4 Next >>

ol	Source Address	Source
	194.90.9.4	NA
	212.150.48.98	47081
	61.66.170.96	4836
	NA	NA
	194.90.9.4	61096
	61.66.170.96	4836
	212.150.48.98	47081
	61.66.170.96	4836
	194.90.9.4	61096
	61.66.170.96	4836

User Define Report

radware

Folders

- User Define Report
  - Device
  - Source Network
  - Destination Network
  - Physical Interface
  - Category
  - Attacks
  - Risk
  - Report Layout
  - Schedule
  - Summary

General

Please enter all parameters that define the network

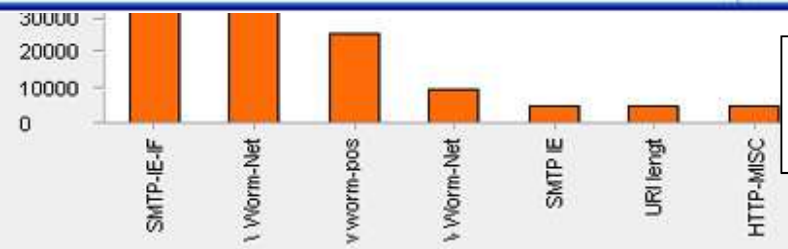
Customer

- Any Customer
- Single Customer Select Custom
- Multiple Customers

Period

- All Days
- Last Day
- From: Jan 1 2004
- To: Jan 1 2004

Next > Cancel



User Defined Reports

Configuration Statistics Security Reports

radware

Management - Executive Reports

radware

Executive Summary
Security Report

Device: 10.204.151.5
Start Date: August 15, 2004 00:00
End Date: August 22, 2004 23:59

Top 10 Attacks

#	Attack Name	Category	Severity
1	Coldfusion file exists	Intrusions	High
2	HTTP/MISC net attempt	Intrusions	Medium
3	CGI www access	Intrusions	High
4	HTTP/MISC mysql admin tool	Intrusions	Medium
5	Backdoor Gate counter	Intrusions	Medium
6	CGI commerce cgi access	Intrusions	Low
7	HTTP/MISC class access	Intrusions	Low
8	CGI test cgi access	Intrusions	Low
9	SCAN syn fin	Anti Scanning	Low
10	Anomaly no flags	Anomalies	Low

radware

radware

Executive Summary
Security Report

Device: 10.204.151.5
Start Date: August 15, 2004 00:00
End Date: August 22, 2004 23:59

Top Attack Source

#	Source	Count
1	10.1.1.22	1240
2	1.1.1.1	887
3	117.149.10.194	687
4	57.88.92.151	665
5	101.228.107	608
6	129.115.26.230	223
7	132.26.99.7	124
8	71.98.18.84	121
9	19.180.183.80	87
10	1.1.1.2	21

radware

radware

Executive Summary
Security Report

Device: 10.204.151.5
Start Date: August 15, 2004 00:00
End Date: August 22, 2004 23:59

Attacks By Risk

- Medium
- Low
- High

#	Attack Risk	Count
1	High	4040
2	Medium	887
3	Low	324

radware

radware

Configware Insite - C:/Documents and Settings/udi/ConfigwareInsite/UserFiles/Untitled.rdw

File Device SynApps General Statistics Help

Dashboard Logs Reports Map

Device: All

Date : 22.12.04 01:30PM Display Last: 10 Hour/s Update

Top Attacks

Total Active Attacks: 5

Worm NetSky-R (1) infection attempt

Worm Mydoom-M attchment detected (3)

Worm Mydoom- A3

Worm Welchia_icmp

Top Sources

194.90.9.4 0 (0%)
194.90.9.4 0 (0%)
194.90.9.4 0 (0%)
194.90.9.4 0 (0%)
194.90.9.4 0 (0%)

Attcks by Risk

high 0 (0%)
medium 0 (0%)
low 0 (0%)
n-a 0 (0%)

Top Target

212.150.43.201 0 (0%)
212.150.43.201 0 (0%)
0 (0%)
194.90.9.4 0 (0%)
194.90.9.4 0 (0%)

Attacks by Groups

Intrusions 0 (0%)
Anomalies 0 (0%)

Last event: Worm NetSky-R, 1000kpps at 5:00 AM

Number of Attacks

New multi device dashboard with live event

Configuration Statistics Security Reports

radware

Configware Insite - Top Attacks Dashboard

File Device SynApps General Statistics Help

radware

Device: All

Date : 22.12.04 01:30PM Display Last: 10 Hour/s

Update

Top Attacks

Alaska;84

Belarus;53

France;11

Mongolia;23

Mexico;45

Libya;65

India;92

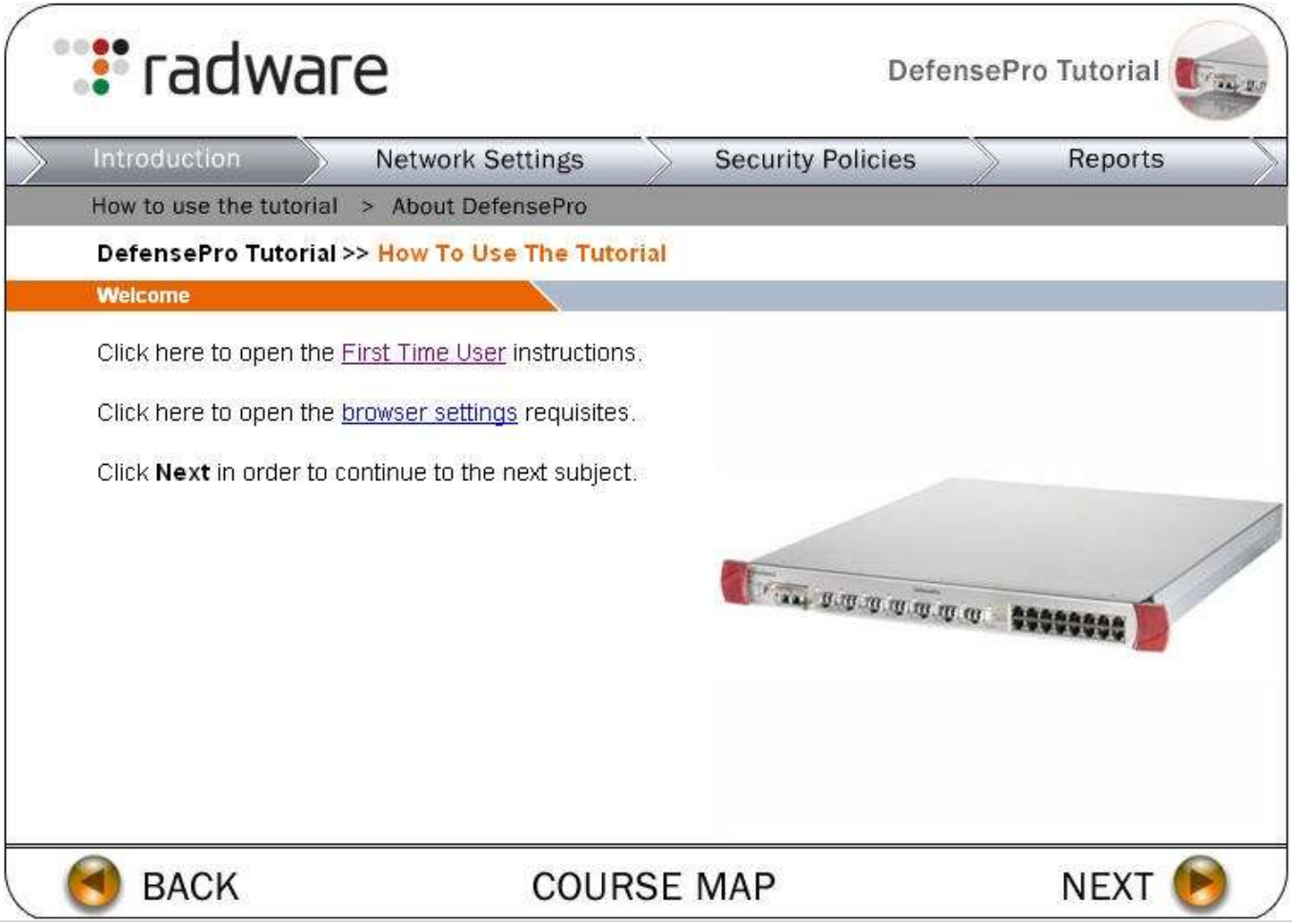
Peru;8

Malawi;38

Geographical map – displays Top Sources according to country of origin

Configuration Statistics Security Reports APM

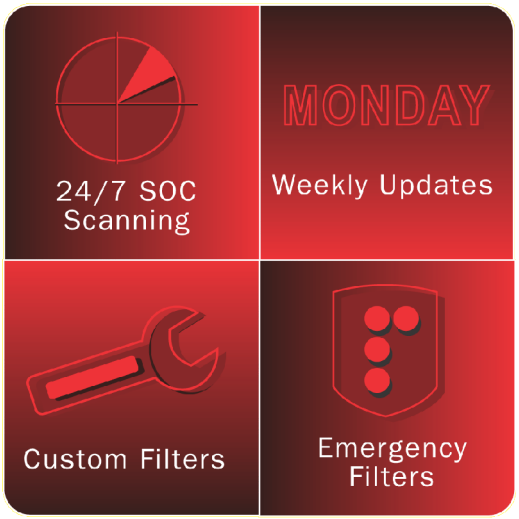
Tutorial


radware
DefensePro Tutorial
Introduction
Network Settings
Security Policies
Reports
How to use the tutorial > About DefensePro
DefensePro Tutorial >> How To Use The Tutorial
Welcome
Click here to open the First Time User instructions.
Click here to open the browser settings requisites.
Click Next in order to continue to the next subject.
BACK
COURSE MAP
NEXT

Security Update Service

Radware DefensePro Solution

- Real Time Update
  - 24/7 operational SoC in Israel and Dallas
  - Shortest time to patch release in the market!



First to Protect!

Sample of Emergency updates that Radware was the first to issue:

MS JPEG Vulnerability, *September 29, 2004*

Mydoom-S, *August 16, 2004*

Bagle-AQ, *August 10, 2004*

Mydoom-M, July 26*, 2004*

Bagle-AG, July 21*, 2004*

Bagle-AB, July 16*, 2004*

AgoBot, *May 17, 2004*

Sasser, *May 3, 2004*

Radware Security Success

France Telecom

Customer requirements: Prevent from Mass mailing attacks (Mydoom A, B) that brought down the Mailing service

Competition: NetScreen IDP (Juniper)

How do we meet the requirements:

- DP successfully blocks Mydoom attack while maintaining mail service
- Allowed the efficient operation of existing mail scanning Anti-virus

Why we won

- Performance

Deployment: 6 Defense Pro 1000 installed in front of France Telecom Email servers

SINA Corporation - China

Customer requirements: Mitigate DoS attacks in real time to ensure on-line gaming operation, reporting

Competition: F5, Netscaler and Nsfocus

How do we meet the requirements:

- Excellent DoS Protection
- Comprehensive reporting

Why we won:

- Outstanding DoS/DDoS protection
- Performance
- QoS ,
- management
- Security Update Service

Deployment:

- 7 DefensePro 3000
- ConfigWare Insight

Deutsche Telekom

Customer requirements: secure VoIP in 60 locations including 2 data centers that have to be available 24*7 hours

Competition: Juniper

Why we won:

- Combination of DOS-protection and IPS
- Performance cababilities
- Multisegment-protection
- Deployment:
- 3 DefensePro 1000
- Potential for many more in the future

Hanaro Carrier Clean Link Security

Radware Secures 3 Million Users from the newest and most damaging viruses

Hanaro Telecom, Inc.

Hanaro is a Leading Korean Telecom

Radware enables:

- Security of all Hanaro users against attacks
- Cleansing attack traffic reducing avg. volume by 170 Mbps
- Eliminated security patch management across POPs

Health Insurance Customer Success

Australian Unity guarantees Perimeter, Core & Branch Security with Radware DefensePro & CAS

Australian Unity is one of Australia's oldest & largest Health Insurance Companies

Radware enables:

- Detection & prevention of security vulnerabilities
- Quality of Service for business critical apps
- Enterprise-wide security solution

Stiff Competition from Incumbents

- Tipping Point

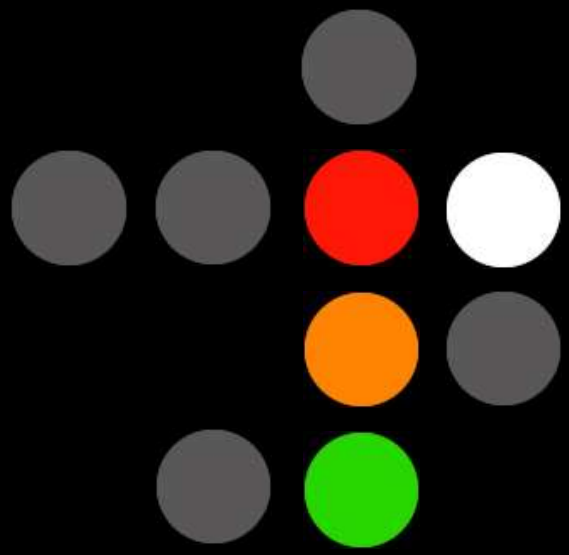
Partnership Development

- Fujitsu

Future Scope

- WSD's & Global load balancing
- Order for additional DP & ~30 x CAS

Questions & Answers



radware

www.radware.com

Summary

NSS Report - April 05

*"Overall, the **performance** of DefensePro is **very good**. Throughput and latency are excellent under almost all network loads and across all packet sizes."*

*"We also found DefensePro to be **very stable**, surviving our extended reliability tests without missing a beat, and **without blocking any legitimate traffic** or succumbing to common evasion techniques."*

Tolly Test

"Tolly Group testing performed on the Radware DefensePro **met and exceeded preliminary expectations.** Our engineers have tested many intrusion prevention products and **DefensePro is notable** because it withstood a battery of real-world attacks and still continued to **deliver a high rate of throughput."**

Kevin Tolly, President/CEO of The Tolly Group. April 2005.

Conclusion

Effective mitigation of DoS attacks requires bi-directional deep packet inspection in order to:

- Block Worms that contains DDoS BOT code
- Mitigate DDoS attacks

Radware's is the **only vendor** that combines advanced **IPS** capabilities with a comprehensive **DDoS mitigation** techniques:

- Real time blocking of DDoS BOT worms
- Protection from all known DoS /DDoS attacks
- Bandwidth Management to shape traffic, block 'unknown' attacks
- SYN Cookies Against ALL SYN Floods

DefensePro Differentiators

3 Gigabit Security Switching Performance

Multi segment protection

Multi discipline Denial of Service Protection

Real time blocking of DDoS BOT worms

Attack isolation and traffic shaping

Continuous operation of mission critical application even during DDoS attack

Why Radware

Market Leader & focused player in security & Application Switching

Pioneering & Award Winning Technologies (1st in Security Switching & Firewall load balancing)

Over 1,800 customers for largest Intrusion Prevention switch install base

Ongoing Security Update Service & Support

Strong Financials

Competitive Landscape

Radware vs. competition

Security requirements	NAI	3com	ISS	Radware
Product	IntruShield 4000	Unity 2400	G-200	DefensePro
performance	2 Gbps	2Gbps	200Mbps	3Gbps
Dedicated HW architecture	Yes	Yes	No (PC based)	Yes
Layer 7 protection	Yes	Yes	Yes	Yes
Advanced DoS protection	No	No	No	Yes
Multi-segment protection	4 GE Limited to 2 segments	4 segments	2+2GbE	7GE +16 FE 11 segments
Protection from SSL based attacks	Yes	No	No	yes
BWM	No	Limited	No	Yes
Real time security update	Yes	yes	yes	yes
Real time visibility	Limited	Unknown	Unknown	Yes
Enable operation of critical application under attack	No	No	No	Yes
Ease of use	Complex	Complex	Medium	Easy (15 minutes installation)

Radware vs. DoS Only players

Both Riverhead and Arbor network suffer from the same limitations:

- Unidirectional protection: only inbound
- No IPS : no ability to block DoS worms such as mydoom
- Relies on Cisco routers : require upgrade of all routers software
- Limited performance : 1G in case of Riverhead, slightly higher in case of arbor
- No Bandwidth Management