COSC130

Intrusion Detection

Uday Tupakula
A/Prof in Cyber Security
School of Science and Technology
Faculty of Science, Agriculture, Business and Law
University of New England

Overview

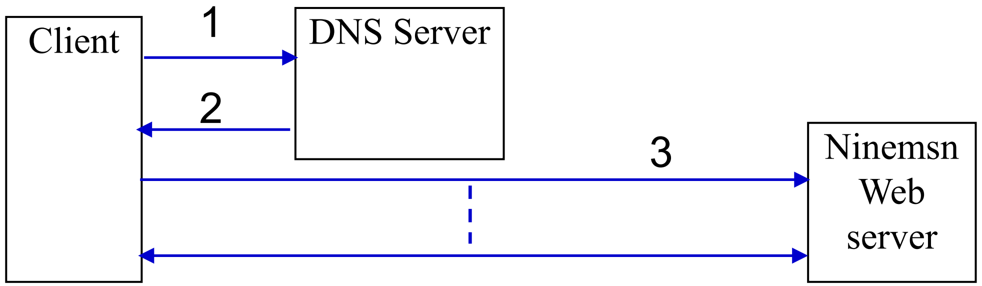
- End to End Communication

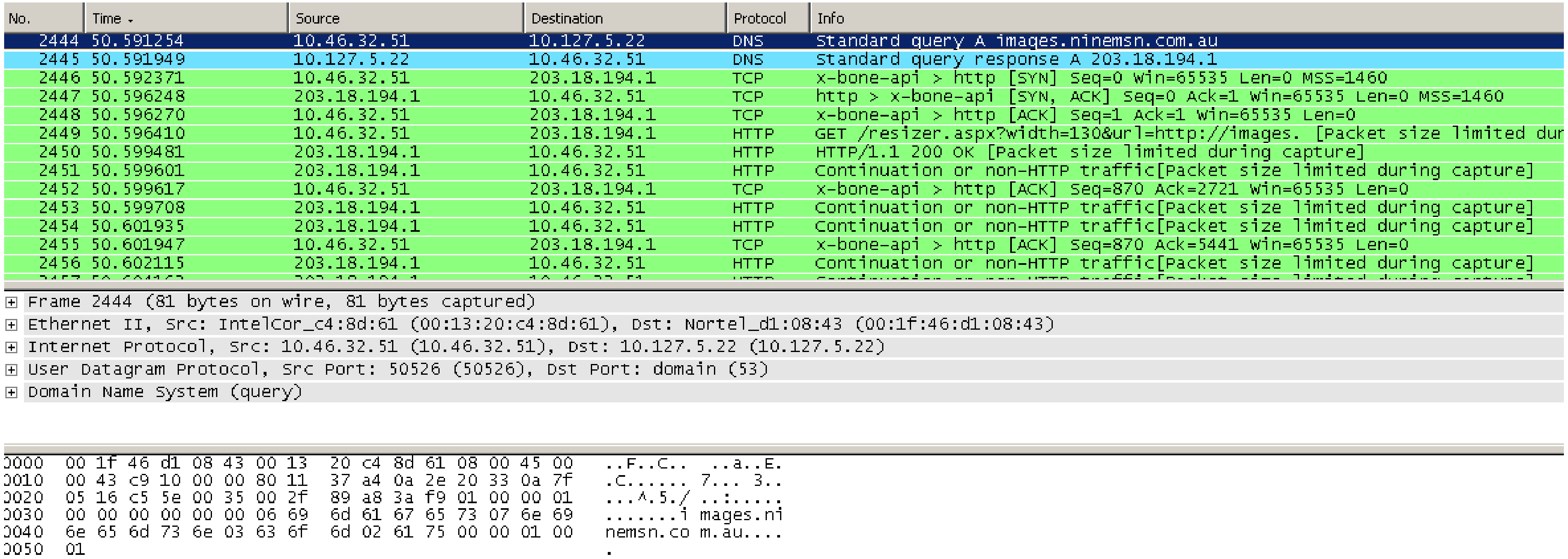
- Firewalls

- Intrusion Detection and Prevention Systems

- Demo

End-to-End Communication





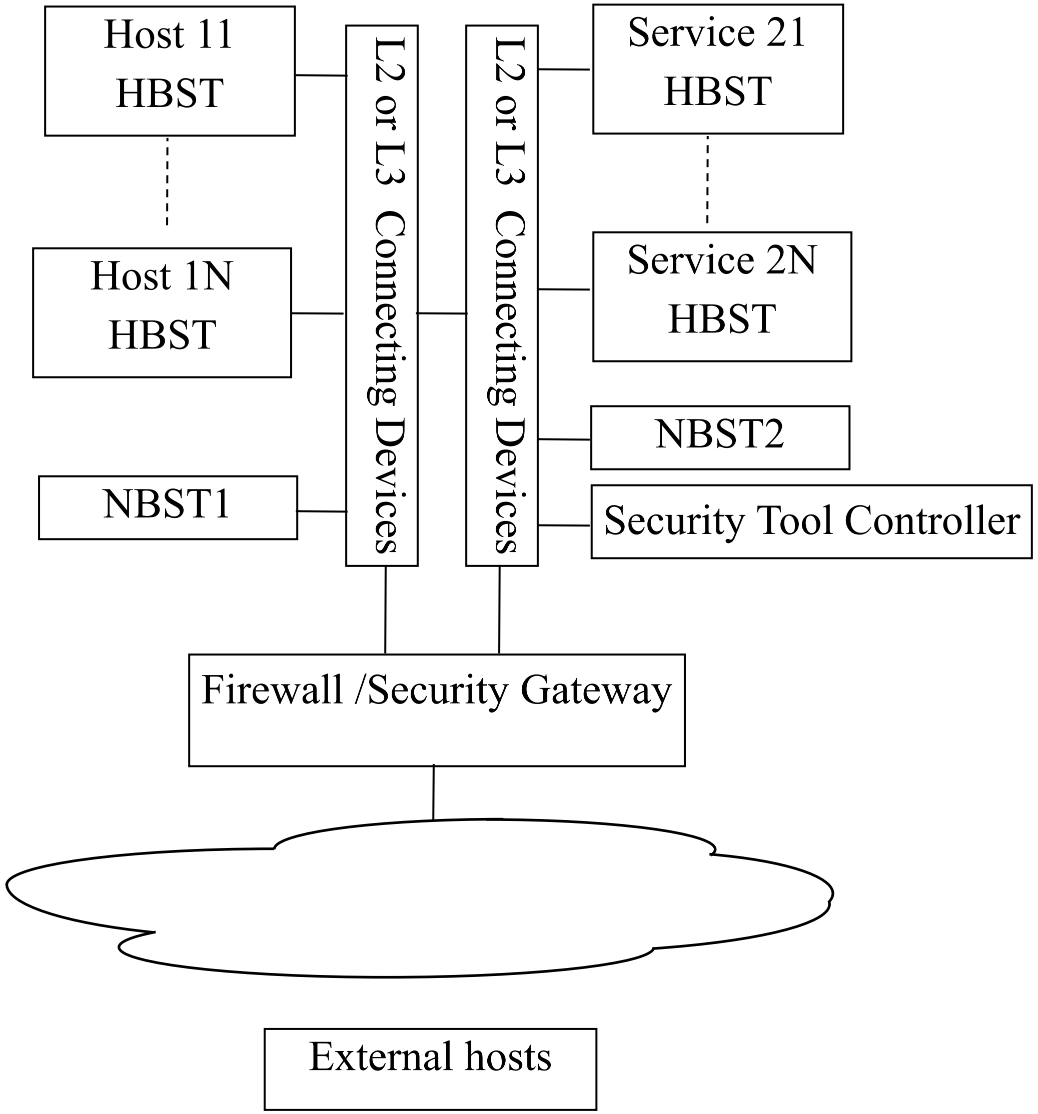
No.	Time	Source	Destination	Protocol	Info
2444	50.591254	10.46.32.51	10.127.5.22	DNS	Standard query A images.ninemsn.com.au
2445	50.591949	10.127.5.22	10.46.32.51	DNS	Standard query response A 203.18.194.1
2446	50.592371	10.46.32.51	203.18.194.1	TCP	x-bone-api > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460
2447	50.596248	203.18.194.1	10.46.32.51	TCP	http > x-bone-api [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
2448	50.596270	10.46.32.51	203.18.194.1	TCP	x-bone-api > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
2449	50.596410	10.46.32.51	203.18.194.1	HTTP	GET /resizer.aspx?width=130&url=http://images. [Packet size limited dur
2450	50.599481	203.18.194.1	10.46.32.51	HTTP	HTTP/1.1 200 OK [Packet size limited during capture]
2451	50.599601	203.18.194.1	10.46.32.51	HTTP	Continuation or non-HTTP traffic[Packet size limited during capture]
2452	50.599617	10.46.32.51	203.18.194.1	TCP	x-bone-api > http [ACK] Seq=870 Ack=2721 Win=65535 Len=0
2453	50.599708	203.18.194.1	10.46.32.51	HTTP	Continuation or non-HTTP traffic[Packet size limited during capture]
2454	50.601935	203.18.194.1	10.46.32.51	HTTP	Continuation or non-HTTP traffic[Packet size limited during capture]
2455	50.601947	10.46.32.51	203.18.194.1	TCP	x-bone-api > http [ACK] Seq=870 Ack=5441 Win=65535 Len=0
2456	50.602115	203.18.194.1	10.46.32.51	HTTP	Continuation or non-HTTP traffic[Packet size limited during capture]

```
⊞ Frame 2444 (81 bytes on wire, 81 bytes captured)
⊞ Ethernet II, Src: IntelCor_c4:8d:61 (00:13:20:c4:8d:61), Dst: Nortel_d1:08:43 (00:1f:46:d1:08:43)
⊞ Internet Protocol, Src: 10.46.32.51 (10.46.32.51), Dst: 10.127.5.22 (10.127.5.22)
⊞ User Datagram Protocol, Src Port: 50526 (50526), Dst Port: domain (53)
⊞ Domain Name System (query)
```

```
0000  00 1f 46 d1 08 43 00 13  20 c4 8d 61 08 00 45 00   ..F..C..  ..a..E.
0010  00 43 c9 10 00 00 80 11  37 a4 0a 2e 20 33 0a 7f   .C...... 7... 3..
0020  05 16 c5 5e 00 35 00 2f  89 a8 3a f9 01 00 00 01   ...^.5./ ..:.....
0030  00 00 00 00 00 00 06 69  6d 61 67 65 73 07 6e 69   .......i mages.ni
0040  6e 65 6d 73 6e 03 63 6f  6d 02 61 75 00 00 01 00   nemsn.co m.au....
0050  01                                                 .
```

Sample Enterprise Network Scenario

- HBST: Host based Security Tool
- NBST: Network based Security Tool



Firewalls

- NIST-SP800-41: Firewalls are devices or programs that control the flow of network traffic between networks or hosts that employ differing security postures.
- Used to enforce organisation security policies
- Different types of firewalls used in the current environment
- Common issues
    - Assuming firewall protects from all the attacks
    - Assuming monitored network to be trusted
    - Not monitoring traffic from protected network
    - Bottleneck

Firewall Policy

- A firewall policy dictates how firewalls should handle network traffic based on the organization’s information security policies

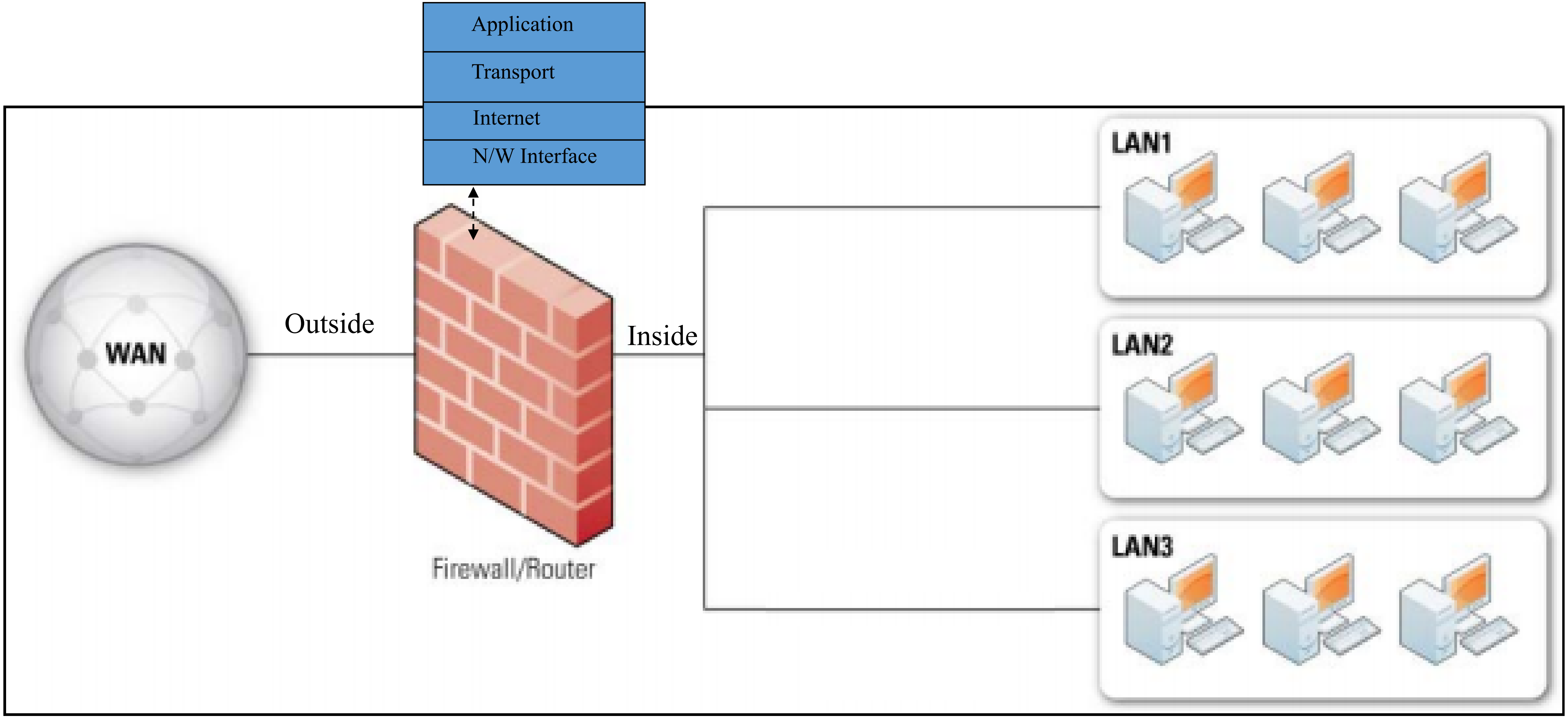
- Create policies based on risk analysis
  - based on what is required and how they must be secured
  - based on threats & impact of attack

- Firewall policy should be documented in the system security plan and maintained and updated regularly

- The policy should also include specific guidance on how to address changes to the ruleset

- Generally, firewalls should block all traffic that has not been expressly permitted by the firewall policy—default deny

Applying Security Policies



Application

Transport

Internet

N/W Interface

Outside

Inside

Packet Filters

- Basic features supported in several security tools

- Also known as stateless packet filters

- Do not maintain the state of the connections

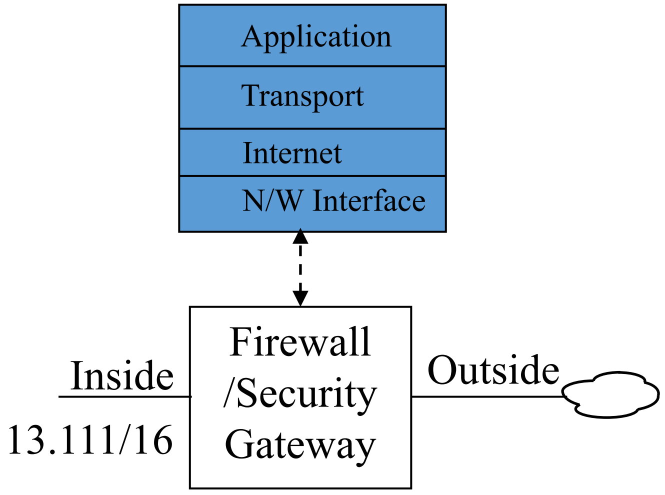
- Traffic allowed or dropped based on first or best match

- Filtering
  - generally performed on MAC and/or IP header and/or transport layer information

  - Traversed interface and direction (inbound/outbound)

Sample Access Control in Packet Filters

Action	Source address	Destination Address	protocol	Source port	Destination port	Flag bit
allow	137.111/16	Outside of 137.111/16	TCP	>1023	80	any
allow	Outside of 137.111/16	137.111/16	TCP	80	>1023	ACK
allow	137.111/16	Outside of 137.111/16	UDP	>1023	53	-
allow	Outside of 137.111/16	137.111/16	UDP	53	>1023	-
deny	all	all	all	all	all	all



Stateful Filters

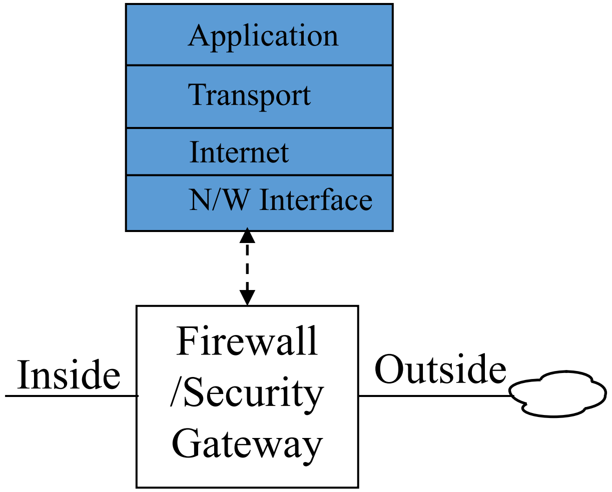
- Maintain state table for the outbound traffic flows

- Flows tracked on the connection state

- Block traffic which deviates expected state

Sample ACL for Stateful Filters

Action	Src.Add	Dest.Add	Protocol	Src.Port	Dest.Prt	Flag bit	Check con
allow	137.111/16	Outside of 137.111/116	TCP	>1023	80	any	
allow	Outside of 137.111/116	137.111/16	TCP	80	>1023	Ack	X
Allow	137.111/16	Outside of 137.111/116	UDP	>1023	53		
Allow	Outside of 137.111/116	137.111/16	UDP	53	>1023		X
Deny	All	All	All	All	All	All	



Source Address	Destination Address	Source port	Destination port	Connection state
137.111.225.5	10.11.12.13	1379	80	initiated
137.111.225.6	200.201.202.203	4825	80	established
137.111.225.7	150.152.1.2	5647	80	established

Application Firewalls

- Can enforce policies from low layer of TCP/IP to top layer (Applications)

- Can monitor user activity or specific inputs
  - Eg: prevent traffic with FTP “put” command
  - Prevent web pages with active content
  - Prevent SSL certificates signed by particular Certification Authority

- Considerable overhead

Intrusion Detection and Prevention Systems(IDPS)

- Process of monitoring systems for different events and analysing for incidents

- Example: Monitor for violation of policies, threat to the systems, acceptable usage policies and detection of attacks

- NIST definition of IDS and IPS

    - An intrusion detection system (IDS) is software that automates the intrusion detection process.

    - An intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents.

Uses of IDPS Technologies

- Primarily focussed on identifying possible incidents
  - Eg: detect an attack & raise an alert to the security admin
- Could log information that can be used by incident handlers
- Can identify reconnaissance activity
- Identifying security problems
- Documenting the existing threat to an organisation
- Deterring individuals from violating security policies

IDPS Overview

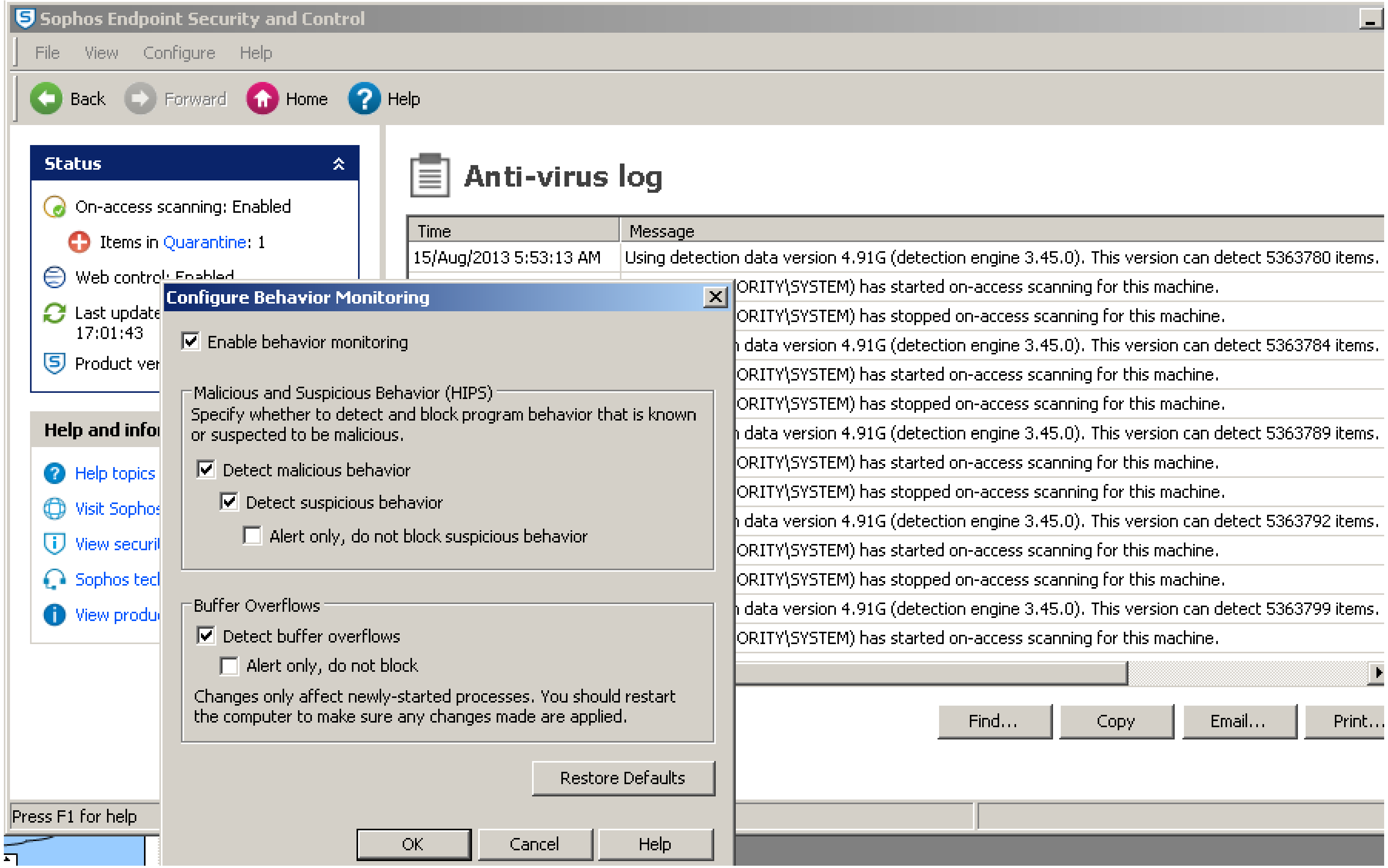
- IDPS Key Functions
  - Record information, raises alerts/notifications, Producing Reports

- IPS responses
  - Stops the attack
  - Changes the security environment
  - Changes the attack content

- Detection Methodologies
  - Signature Based
  - Anomaly Based

- Types of IDPS
  - Host Based, Network Based (and Wireless*)

IDS and IPS



On-access scanning: Enabled
Items in Quarantine: 1
Web control: Enabled
Last update 17:01:43
Product ver

Anti-virus log

```
Time                   Message
15/Aug/2013 5:53:13 AM Using detection data version 4.91G (detection engine 3.45.0). This version can detect 5363780 items.
                       ORITY\SYSTEM) has started on-access scanning for this machine.
                       ORITY\SYSTEM) has stopped on-access scanning for this machine.
                       data version 4.91G (detection engine 3.45.0). This version can detect 5363784 items.
                       ORITY\SYSTEM) has started on-access scanning for this machine.
                       ORITY\SYSTEM) has stopped on-access scanning for this machine.
                       data version 4.91G (detection engine 3.45.0). This version can detect 5363789 items.
                       ORITY\SYSTEM) has started on-access scanning for this machine.
                       ORITY\SYSTEM) has stopped on-access scanning for this machine.
                       data version 4.91G (detection engine 3.45.0). This version can detect 5363792 items.
                       ORITY\SYSTEM) has started on-access scanning for this machine.
                       ORITY\SYSTEM) has stopped on-access scanning for this machine.
                       data version 4.91G (detection engine 3.45.0). This version can detect 5363799 items.
                       ORITY\SYSTEM) has started on-access scanning for this machine.
```

Configure Behavior Monitoring

☑ Enable behavior monitoring

Malicious and Suspicious Behavior (HIPS)

Specify whether to detect and block program behavior that is known or suspected to be malicious.

☑ Detect malicious behavior

☑ Detect suspicious behavior

□ Alert only, do not block suspicious behavior

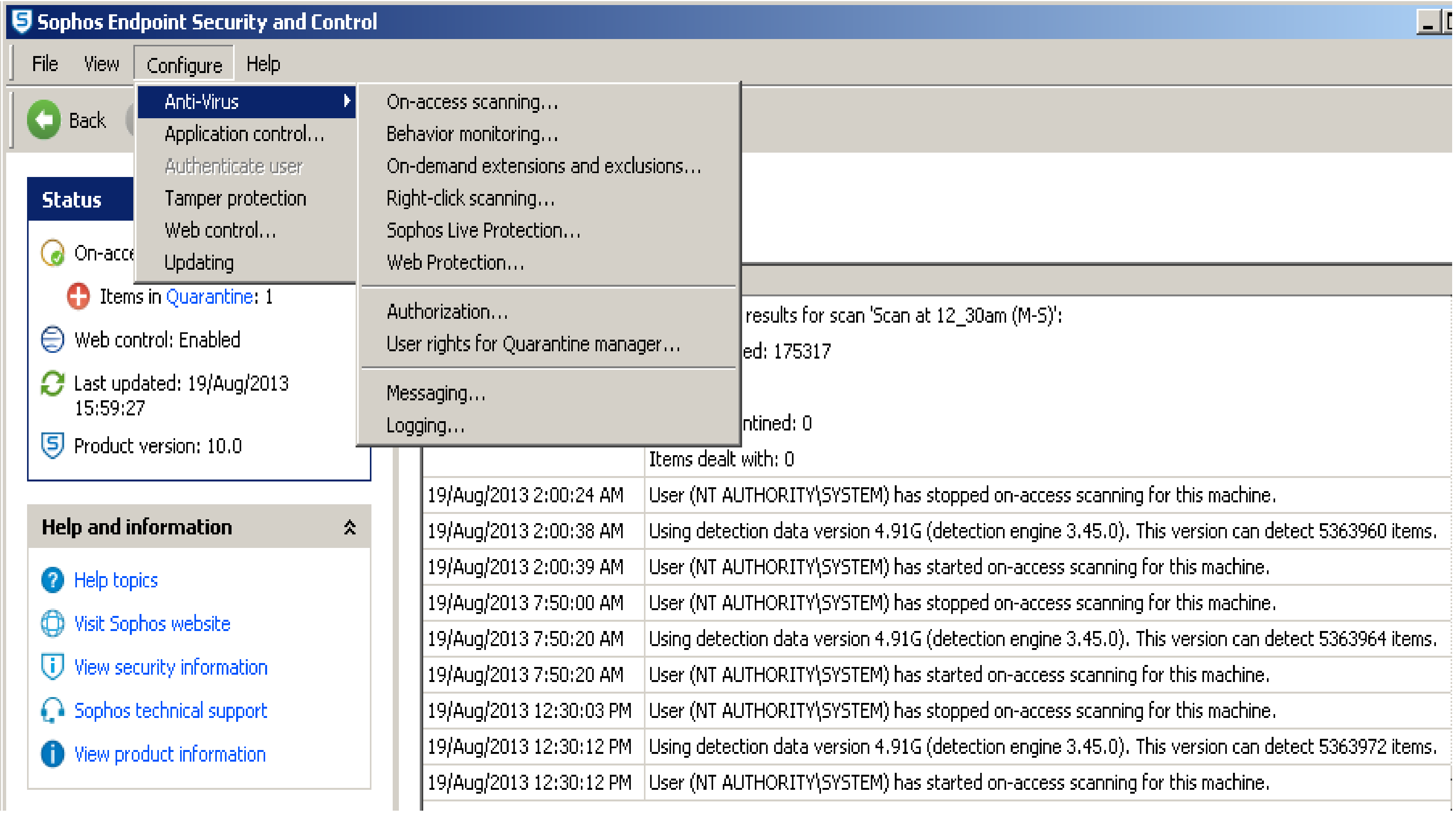
Buffer Overflows

☑ Detect buffer overflows

□ Alert only, do not block

Changes only affect newly-started processes. You should restart the computer to make sure any changes made are applied.

IDS and IPS



Items in Quarantine: 1

Web control: Enabled

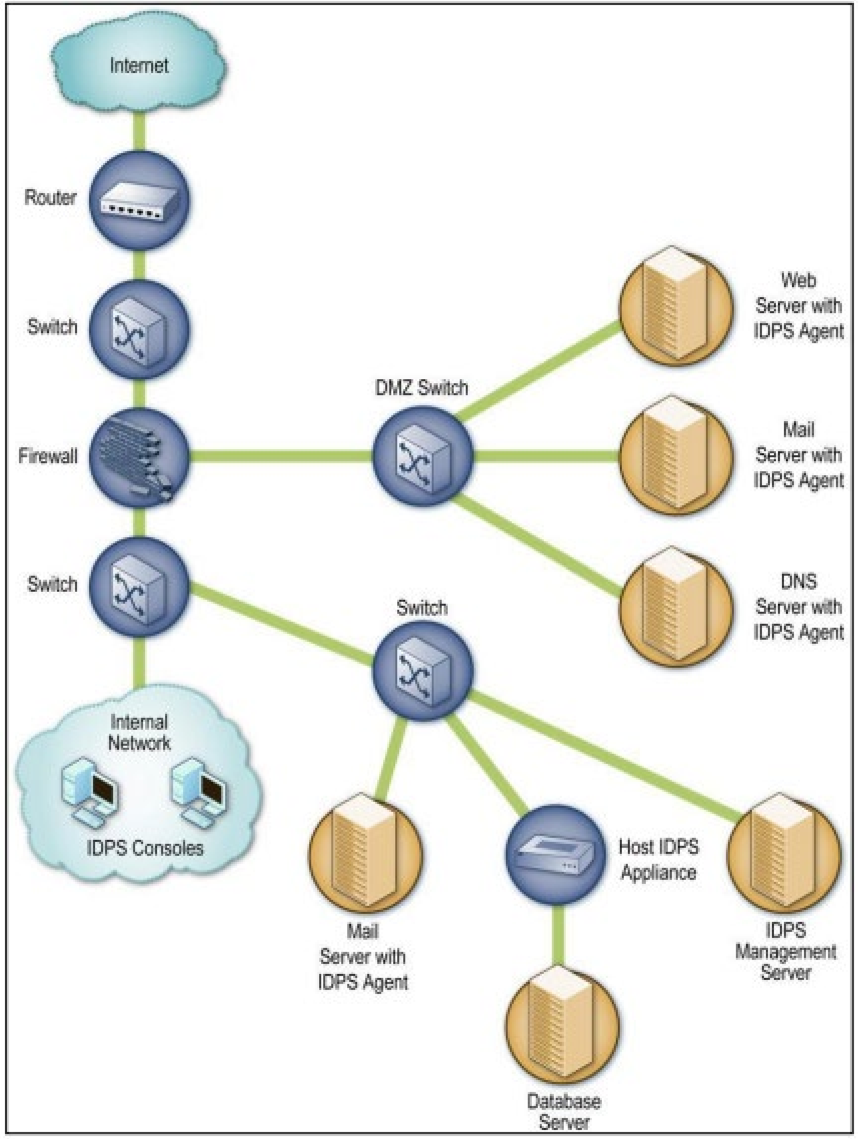
Last updated: 19/Aug/2013 15:59:27

Product version: 10.0

```
                               results for scan 'Scan at 12_30am (M-S)':
                               ed: 175317

                               ntined: 0
                               Items dealt with: 0
19/Aug/2013 2:00:24 AM    User (NT AUTHORITY\SYSTEM) has stopped on-access scanning for this machine.
19/Aug/2013 2:00:38 AM    Using detection data version 4.91G (detection engine 3.45.0). This version can detect 5363960 items.
19/Aug/2013 2:00:39 AM    User (NT AUTHORITY\SYSTEM) has started on-access scanning for this machine.
19/Aug/2013 7:50:00 AM    User (NT AUTHORITY\SYSTEM) has stopped on-access scanning for this machine.
19/Aug/2013 7:50:20 AM    Using detection data version 4.91G (detection engine 3.45.0). This version can detect 5363964 items.
19/Aug/2013 7:50:20 AM    User (NT AUTHORITY\SYSTEM) has started on-access scanning for this machine.
19/Aug/2013 12:30:03 PM   User (NT AUTHORITY\SYSTEM) has stopped on-access scanning for this machine.
19/Aug/2013 12:30:12 PM   Using detection data version 4.91G (detection engine 3.45.0). This version can detect 5363972 items.
19/Aug/2013 12:30:12 PM   User (NT AUTHORITY\SYSTEM) has started on-access scanning for this machine.
```

Host Based IDPS



Host Based IDPS

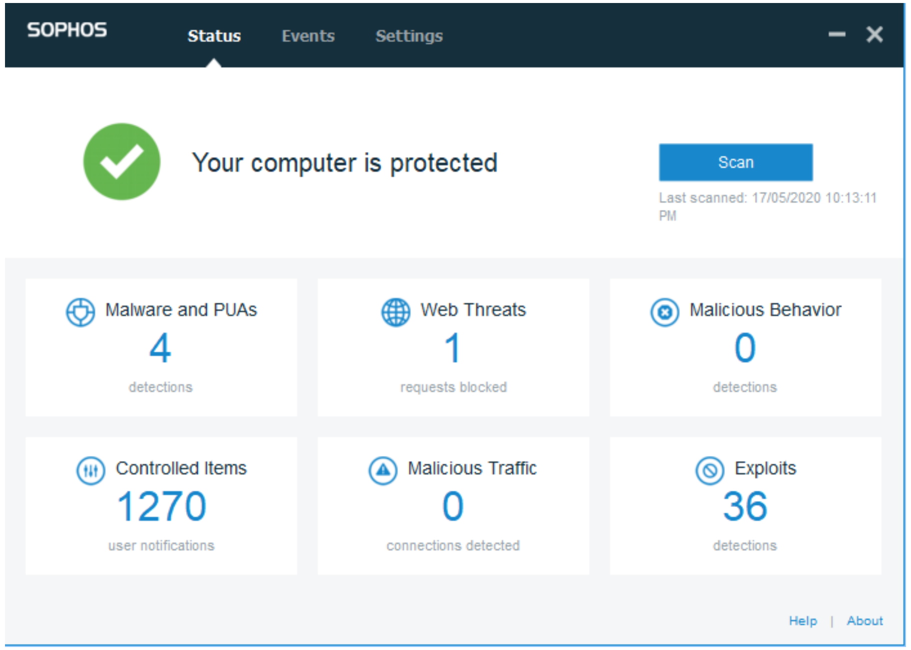
- Generally relates to any Host based Security Tool (HBST)
  - Firewalls, Anti-virus, Intrusion detection systems

- Implemented on all monitored hosts

- Detects attacks by monitoring different activities
  - System processes, access or changes to sensitive files, user activity, and network activity.

- Can be signature based and/or anomaly based

Current Sophos Tool

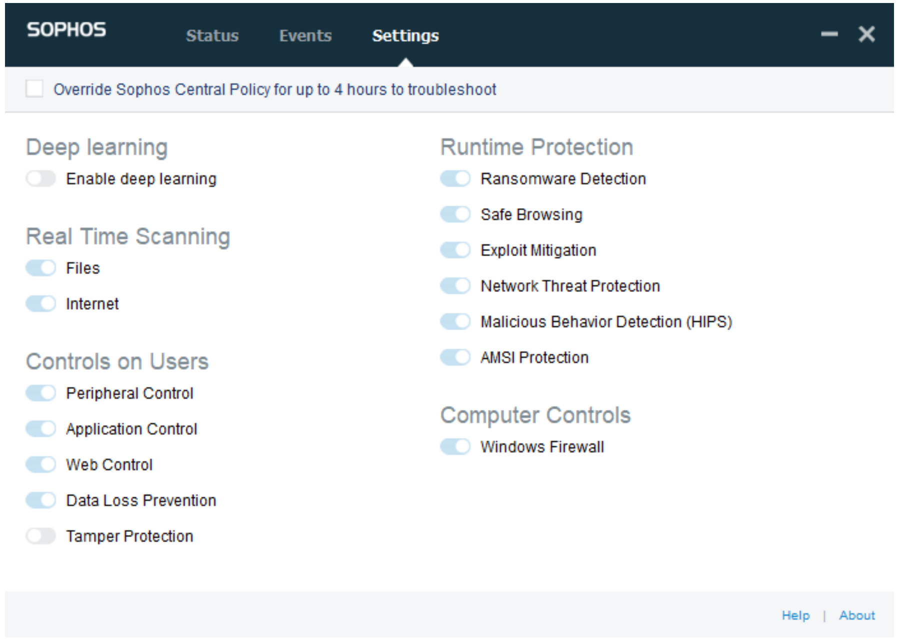


Your computer is protected

Last scanned: 17/05/2020 10:13:11 PM

Malware and PUAs	Web Threats	Malicious Behavior
4 detections	1 requests blocked	0 detections

Controlled Items	Malicious Traffic	Exploits
1270 user notifications	0 connections detected	36 detections



☐ Override Sophos Central Policy for up to 4 hours to troubleshoot

Deep learning
- Enable deep learning

Real Time Scanning
- Files
- Internet

Controls on Users
- Peripheral Control
- Application Control
- Web Control
- Data Loss Prevention
- Tamper Protection

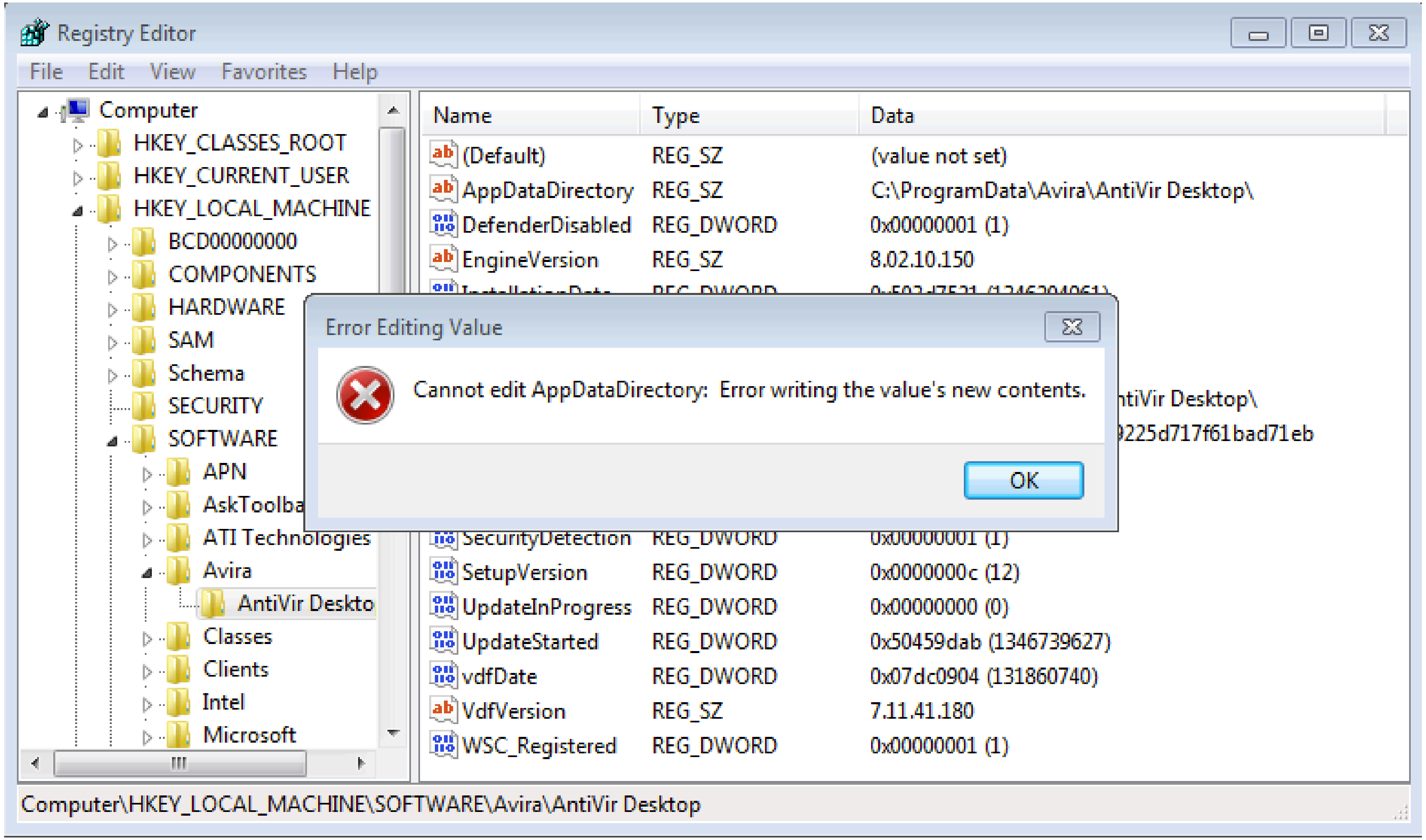
Runtime Protection
- Ransomware Detection
- Safe Browsing
- Exploit Mitigation
- Network Threat Protection
- Malicious Behavior Detection (HIPS)
- AMSI Protection

Computer Controls
- Windows Firewall

Host Based IDPS

- Good visibility of the monitored system
- Good attack detection
- Weak isolation between the monitored host & the security tool
- Emerging attacks disable security tools in the infected system

Self Protection in HBST

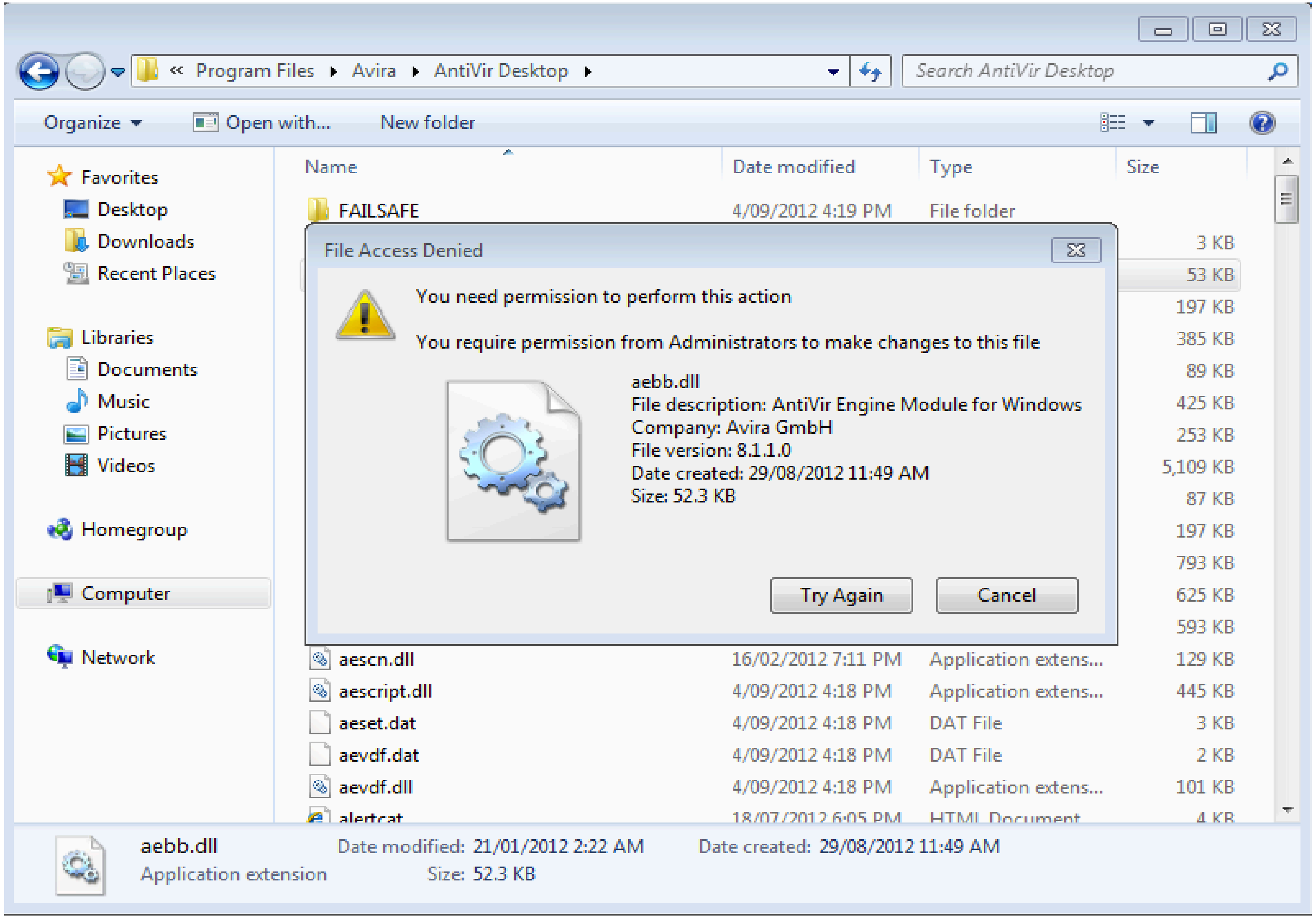


Name	Type	Data
(Default)	REG_SZ	(value not set)
AppDataDirectory	REG_SZ	C:\ProgramData\Avira\AntiVir Desktop\
DefenderDisabled	REG_DWORD	0x00000001 (1)
EngineVersion	REG_SZ	8.02.10.150
InstallationDate	REG_DWORD	0x503d7521 (1346204961)
		tiVir Desktop\
		225d717f61bad71eb
SecurityDetection	REG_DWORD	0x00000001 (1)
SetupVersion	REG_DWORD	0x0000000c (12)
UpdateInProgress	REG_DWORD	0x00000000 (0)
UpdateStarted	REG_DWORD	0x50459dab (1346739627)
vdfDate	REG_DWORD	0x07dc0904 (131860740)
VdfVersion	REG_SZ	7.11.41.180
WSC_Registered	REG_DWORD	0x00000001 (1)

Cannot edit AppDataDirectory: Error writing the value's new contents.

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Avira\AntiVir Desktop

Self Protection in HBST



Name	Date modified	Type	Size
FAILSAFE	4/09/2012 4:19 PM	File folder	
			3 KB
			53 KB
			197 KB
			385 KB
			89 KB
			425 KB
			253 KB
			5,109 KB
			87 KB
			197 KB
			793 KB
			625 KB
			593 KB
aescn.dll	16/02/2012 7:11 PM	Application extens...	129 KB
aescript.dll	4/09/2012 4:18 PM	Application extens...	445 KB
aeset.dat	4/09/2012 4:18 PM	DAT File	3 KB
aevdf.dat	4/09/2012 4:18 PM	DAT File	2 KB
aevdf.dll	4/09/2012 4:18 PM	Application extens...	101 KB
alertcat	18/07/2012 6:05 PM	HTML Document	4 KB

File Access Denied

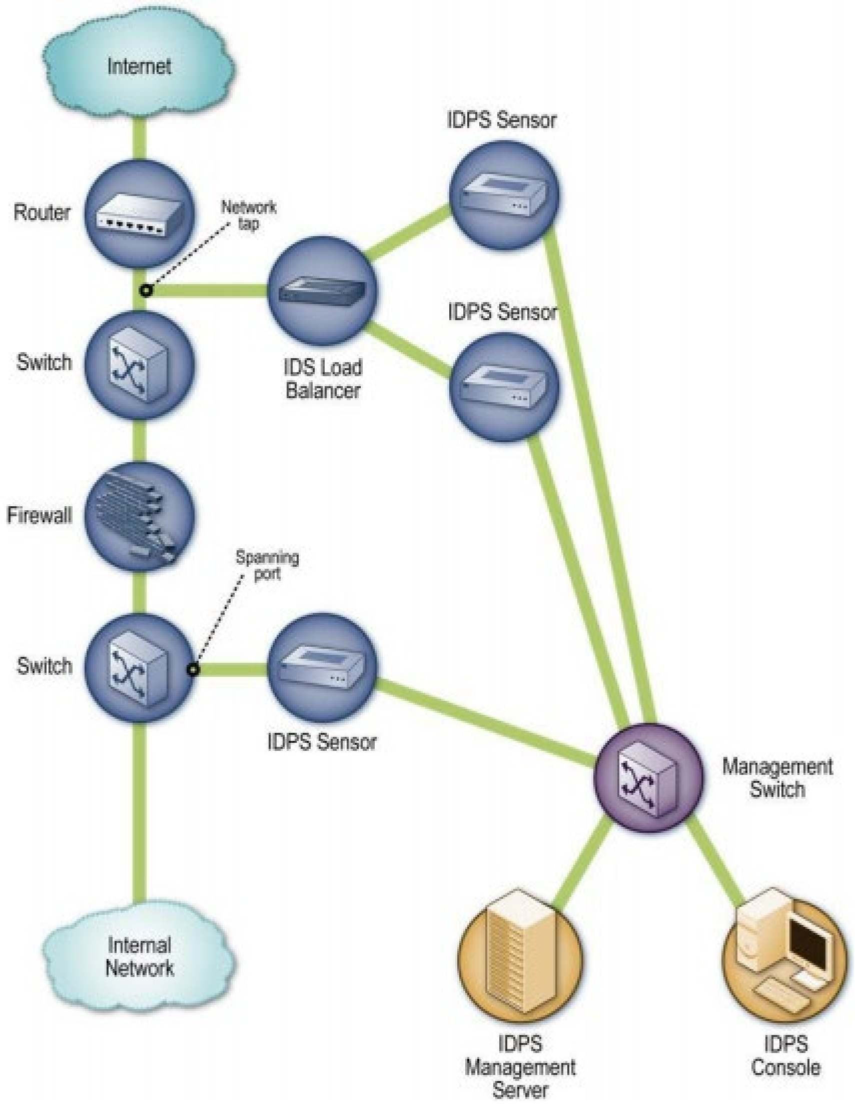
You need permission to perform this action

You require permission from Administrators to make changes to this file

aebb.dll
File description: AntiVir Engine Module for Windows
Company: Avira GmbH
File version: 8.1.1.0
Date created: 29/08/2012 11:49 AM
Size: 52.3 KB

aebb.dll
Application extension
Date modified: 21/01/2012 2:22 AM
Size: 52.3 KB
Date created: 29/08/2012 11:49 AM

Network Based IDPS



Network Based Security Tools

- The security tool can monitor multiple hosts
- Can be signature based and/or anomaly based
- Promiscuous mode of operation
- Detect the attacks by monitoring the host/subnet traffic
  - Port scans, flooding attacks, TCP resets
- Poor visibility of the monitored hosts
- Strong isolation from the monitored hosts
- Challenging to detect attacks with encrypted traffic

Network Based Security Tool Components

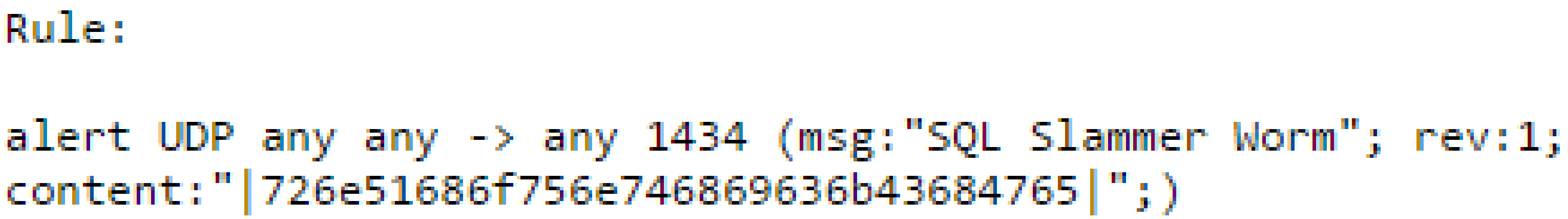
- Load Balancer: to distribute the traffic to multiple sensors
- Sensors: receive traffic from live network or from load balancer
- Database: knowledge repository
- Analyser: makes use of knowledge repository to analyse data from sensor and determine the threats
- Alert Notifier: on screen, alert to admin, paging, email
- Controller: central authority for entire system, configure policies
- Response: take action based on the threat

Signature Based Security Tools

- Attack patterns/signatures are developed for known attacks
- Detect attacks by matching the host activity with the patterns
- Requires frequent update of signatures
- Generally better performance, less false positives & false negatives
- Cannot detect zero day attacks
- Issues identifying exact signature (polymorphism, metamorphism)

Signature Based Security Tools

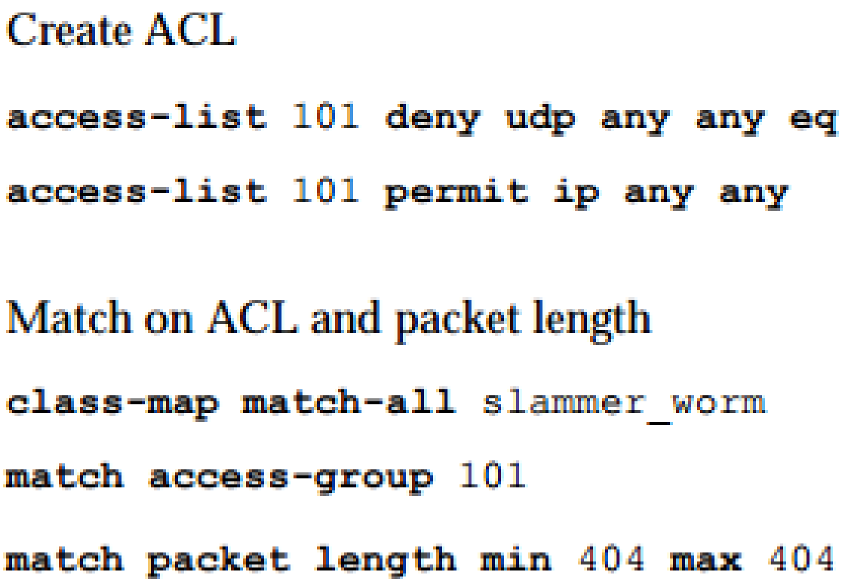
- Snort



```
Rule:

alert UDP any any -> any 1434 (msg:"SQL Slammer Worm"; rev:1;
content:"|726e51686f756e746869636b43684765|";)
```

- Cisco



Create ACL

```
access-list 101 deny udp any any eq 1434
access-list 101 permit ip any any
```

Match on ACL and packet length

```
class-map match-all slammer_worm
match access-group 101
match packet length min 404 max 404
```

Anomaly Based Security Tools

- Behaviour of the monitored users/system/network used for detecting attacks (example: threshold and profile)

- Variation from normal behaviour considered as suspicious activity

- Can detect zero day attacks

- More false alarms

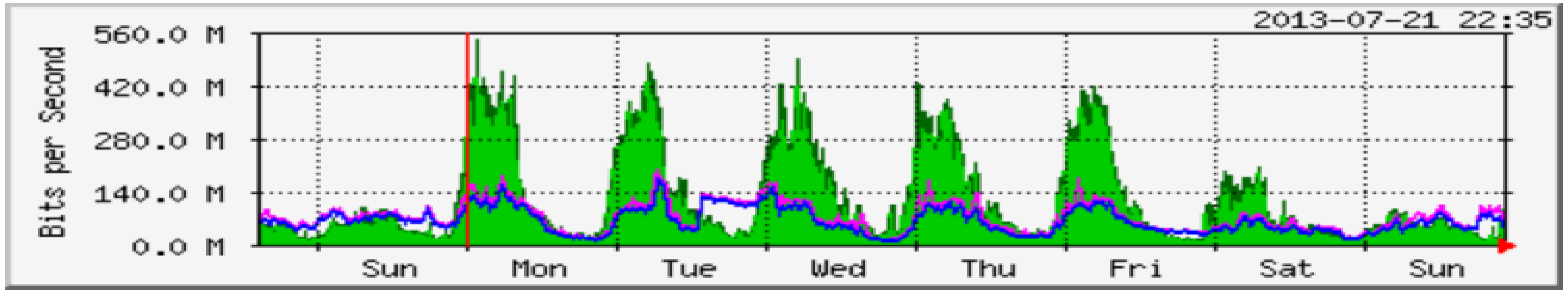
Analysing Traffic Behaviour

- In this case baseline of the traffic is created during the training period

- The deviation of the traffic behaviour from baseline behaviour is used for detecting suspicious activity

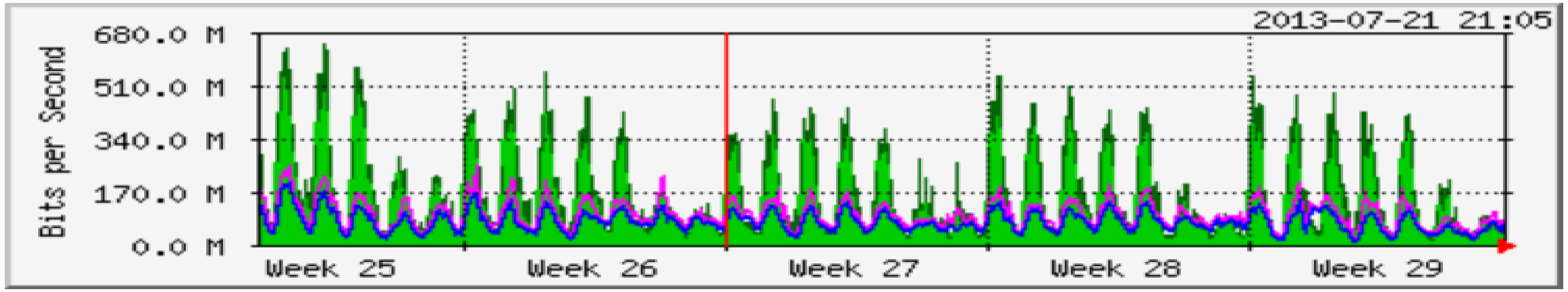
Example: Network Traffic Usage Statistics

`Weekly' Graph (30 Minute Average)



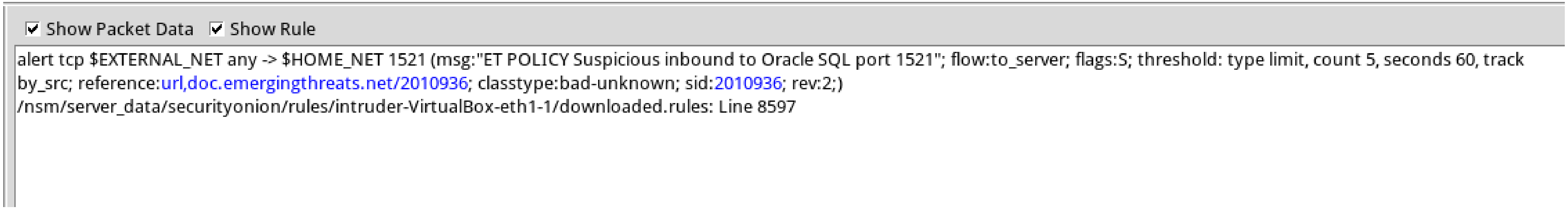
	Max	Average	Current
In	540.0 Mb/s (54.0%)	108.3 Mb/s (10.8%)	91.5 Mb/s (9.1%)
Out	190.9 Mb/s (19.1%)	59.9 Mb/s (6.0%)	32.6 Mb/s (3.3%)

`Monthly' Graph (2 Hour Average)



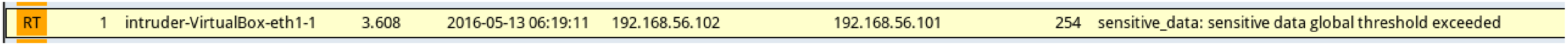
	Max	Average	Current
In	641.6 Mb/s (64.2%)	136.0 Mb/s (13.6%)	12.5 Mb/s (1.3%)
Out	251.3 Mb/s (25.1%)	69.9 Mb/s (7.0%)	76.1 Mb/s (7.6%)

Example: Anomaly Detection



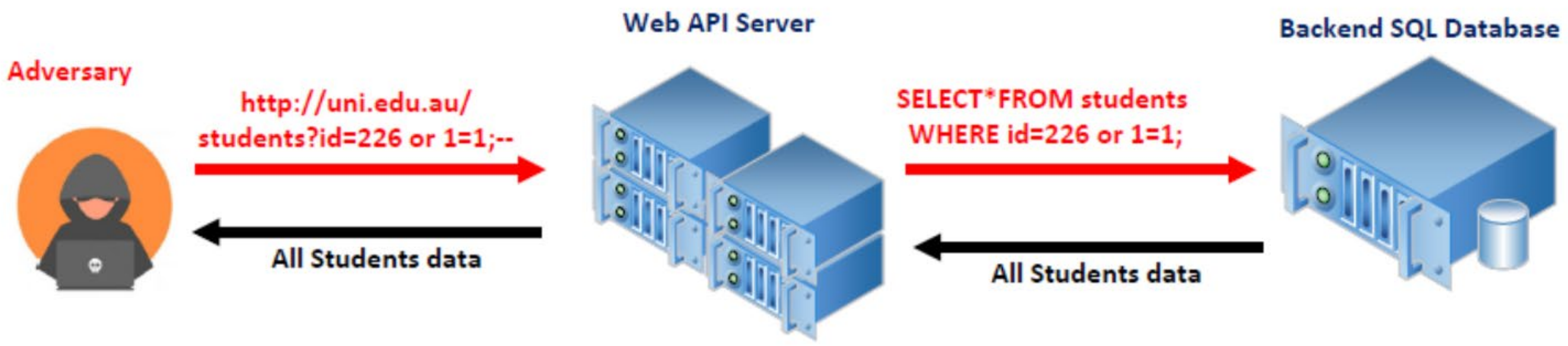
☑ Show Packet Data ☑ Show Rule

```
alert tcp $EXTERNAL_NET any -> $HOME_NET 1521 (msg:"ET POLICY Suspicious inbound to Oracle SQL port 1521"; flow:to_server; flags:S; threshold: type limit, count 5, seconds 60, track
by_src; reference:url,doc.emergingthreats.net/2010936; classtype:bad-unknown; sid:2010936; rev:2;)
/nsm/server_data/securityonion/rules/intruder-VirtualBox-eth1-1/downloaded.rules: Line 8597
```



```
RT    1   intruder-VirtualBox-eth1-1   3.608   2016-05-13 06:19:11   192.168.56.102   192.168.56.101   254   sensitive_data: sensitive data global threshold exceeded
```

SQL Injection



- Common vulnerable login query

  SELECT * FROM users

  WHERE user id = ‘uday’

  AND password = ‘A/cPasw0rd$’

- Use the following values for attack

  user id = ' or 1=1 – –

  password = anything

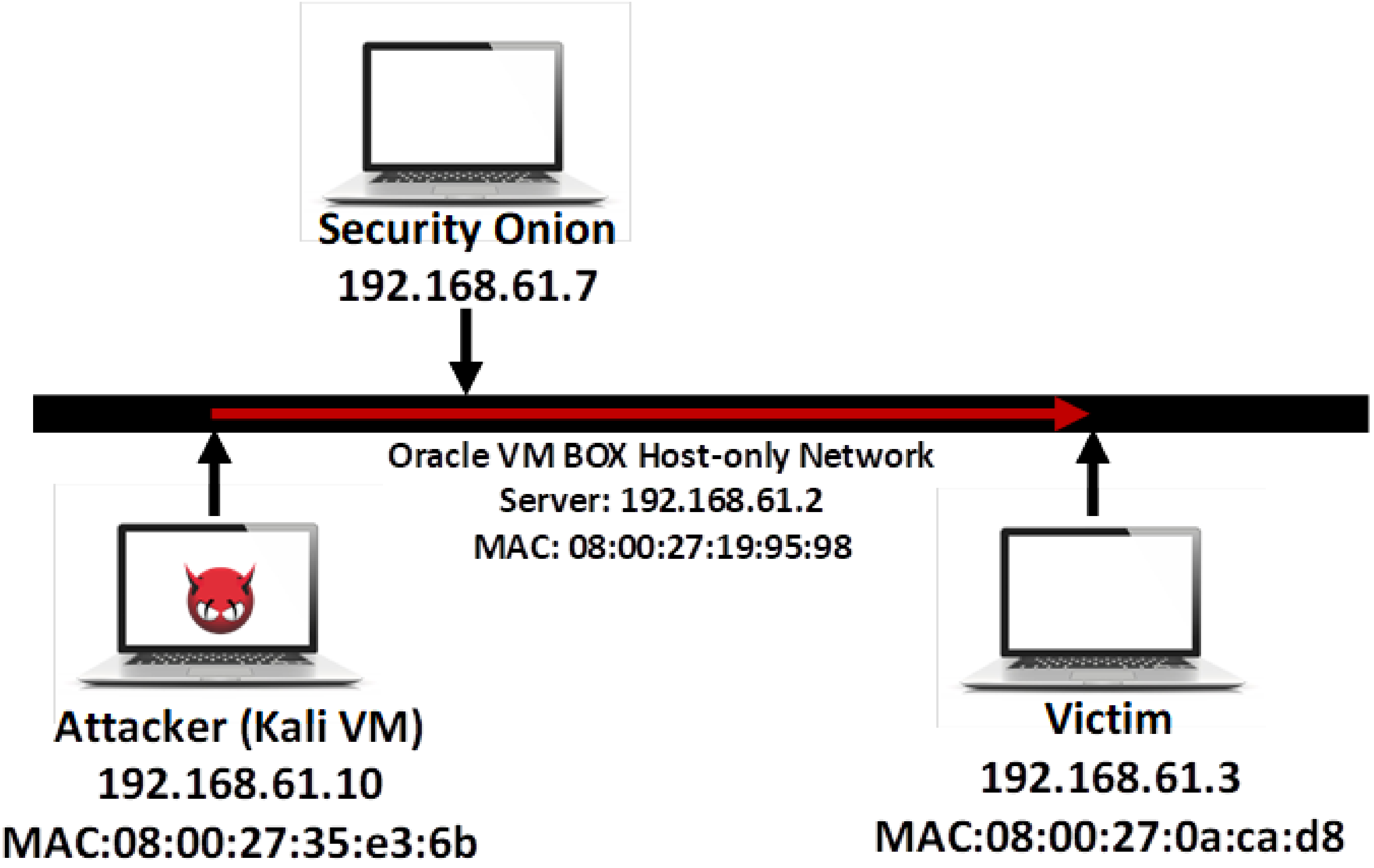
- Final query would look like this:

  SELECT * FROM users

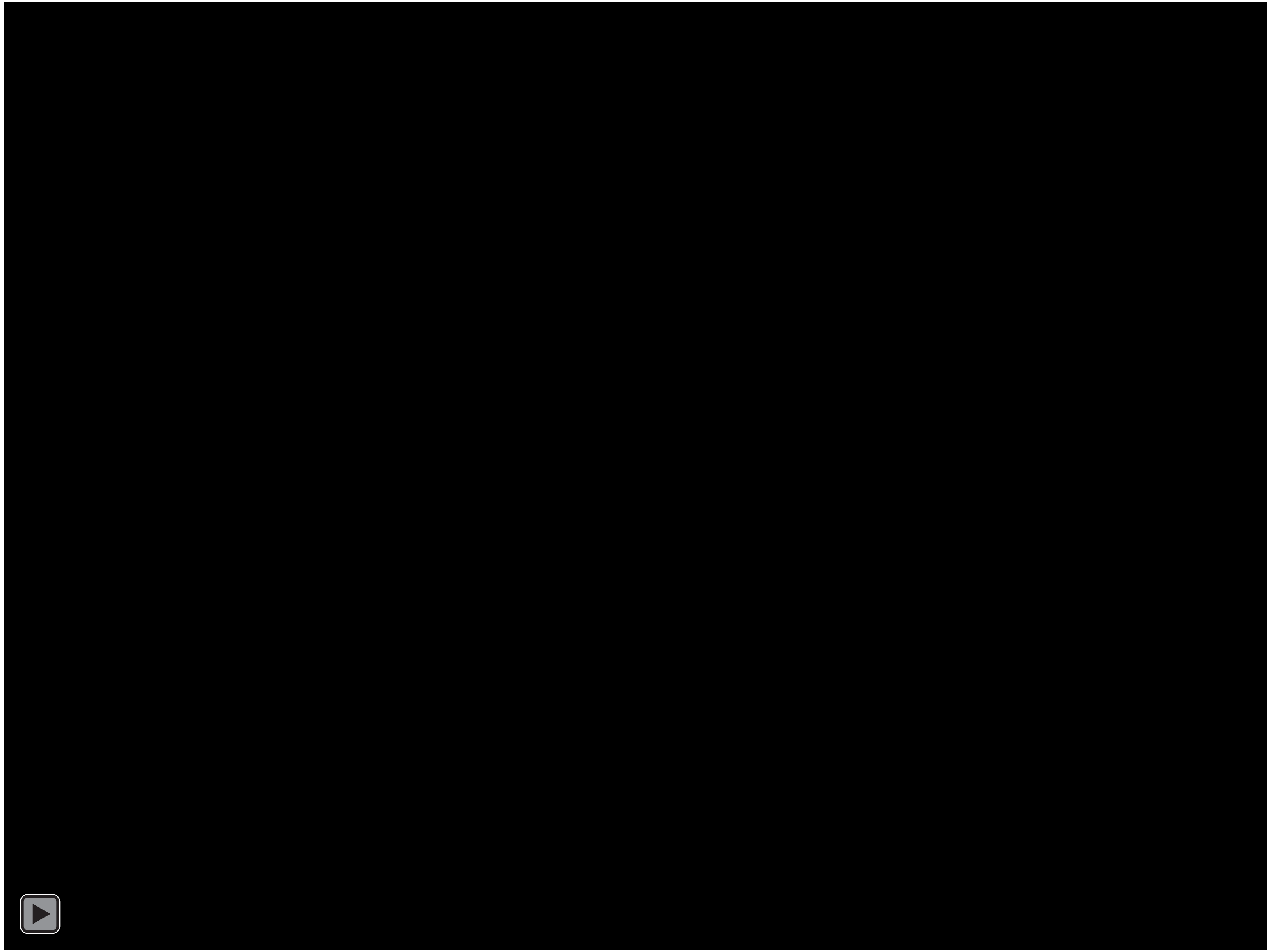
  WHERE user id = ' ' or 1=1

  – – AND password = 'anything'

Attack Generation and Intrusion Detection



Attack Generation and Intrusion Detection



Reading Material

- Guidelines on Firewalls and Firewall Policy
  - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

- Guide to Intrusion Detection and Prevention system
  - https://csrc.nist.gov/CSRC/media/Publications/sp/800-94/rev-1/draft/documents/draft_sp800-94-rev1.pdf