Lesson 10

Implementing Network Security Appliances

CompTIA®

Topic 10A

Implement Firewalls and Proxy Servers

Syllabus Objectives Covered

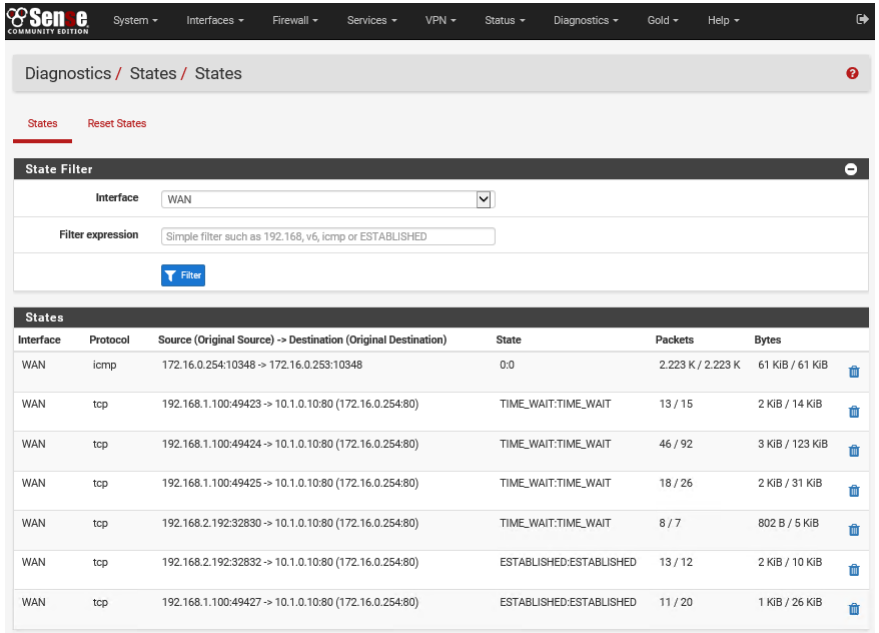
- 3.3 Given a scenario, implement secure network designs

Packet Filtering Firewalls

- Enforce a network access control list (ACL)
- Act to deny (block or drop), log, or accept a packet
- Inspect headers of individual packets
  - Source and destination IP address
  - Protocol ID/type (TCP, UDP, ICMP, routing protocols, and so on)
  - Source and destination port numbers (TCP or UDP application type)
- Inbound, outbound, or both
- Stateless operation

Stateful Inspection Firewalls

- State table stores connection information
- Transport layer (layer 4)
  - TCP handshake
  - New versus established and related connections
- Application layer (layer 7)
  - Validate protocol
  - Match threat signatures
  - Application-specific filtering



Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes
WAN	icmp	172.16.0.254:10348 -> 172.16.0.253:10348	0:0	2.223 K / 2.223 K	61 KiB / 61 KiB
WAN	tcp	192.168.1.100:49423 -> 10.1.0.10:80 (172.16.0.254:80)	TIME_WAIT:TIME_WAIT	13 / 15	2 KiB / 14 KiB
WAN	tcp	192.168.1.100:49424 -> 10.1.0.10:80 (172.16.0.254:80)	TIME_WAIT:TIME_WAIT	46 / 92	3 KiB / 123 KiB
WAN	tcp	192.168.1.100:49425 -> 10.1.0.10:80 (172.16.0.254:80)	TIME_WAIT:TIME_WAIT	18 / 26	2 KiB / 31 KiB
WAN	tcp	192.168.2.192:32830 -> 10.1.0.10:80 (172.16.0.254:80)	TIME_WAIT:TIME_WAIT	8 / 7	802 B / 5 KiB
WAN	tcp	192.168.2.192:32832 -> 10.1.0.10:80 (172.16.0.254:80)	ESTABLISHED:ESTABLISHED	13 / 12	2 KiB / 10 KiB
WAN	tcp	192.168.1.100:49427 -> 10.1.0.10:80 (172.16.0.254:80)	ESTABLISHED:ESTABLISHED	11 / 20	1 KiB / 26 KiB

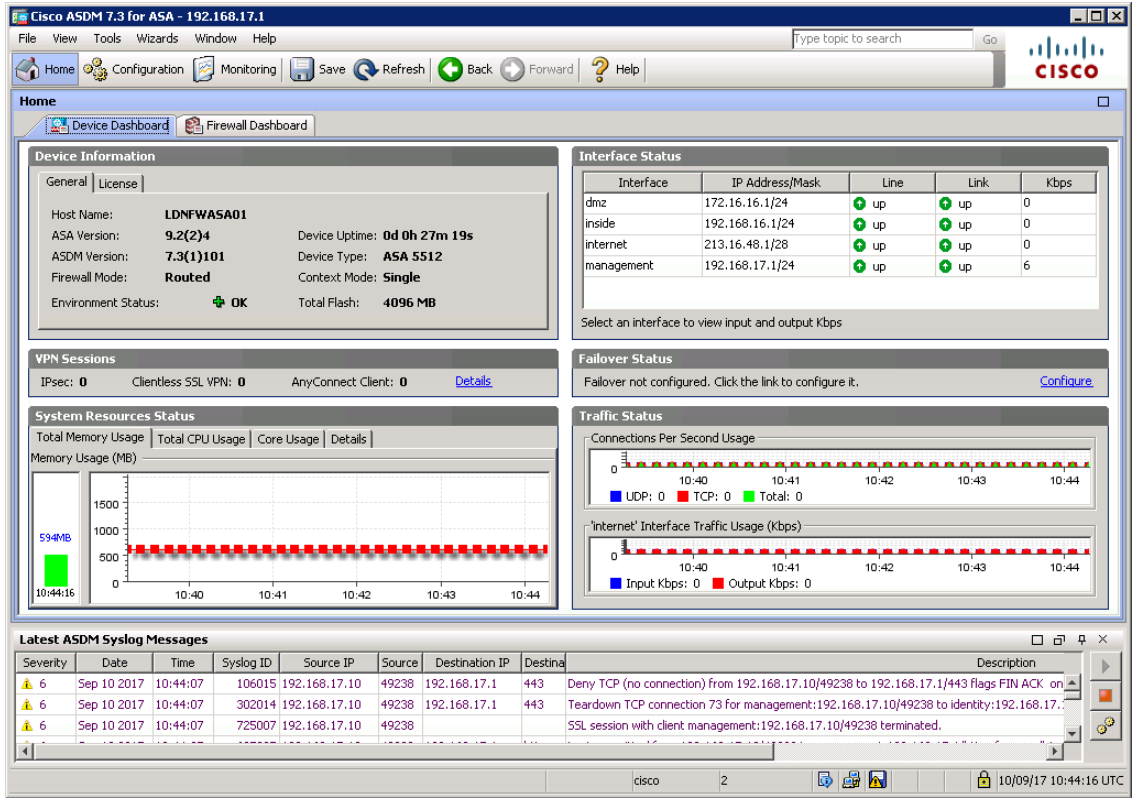
Screenshot used with permission from Rubicon Communications, LLC

iptables

```
Chain INPUT (policy DROP)
num  target    prot  opt  source          destination
1    DROP      all   --   10.1.0.192      0.0.0.0/0
2    ACCEPT    icmp  --   10.1.0.0/24     0.0.0.0/0      icmptype 8
3    ACCEPT    udp   --   0.0.0.0/0       0.0.0.0/0      udp dpt:53
4    ACCEPT    tcp   --   0.0.0.0/0       0.0.0.0/0      tcp dpt:53
5    ACCEPT    tcp   --   10.1.0.0/24     0.0.0.0/0      tcp dpt:80
6    ACCEPT    tcp   --   10.1.0.0/24     0.0.0.0/0      tcp dpt:443
7    ACCEPT    all   --   0.0.0.0/0       0.0.0.0/0      ctstate RELATED,ESTABLISHED
[i@host]$ iptables -I INPUT 2 -p tcp -s 10.1.0.0/24 --dport 22 -j ACCEPT
```

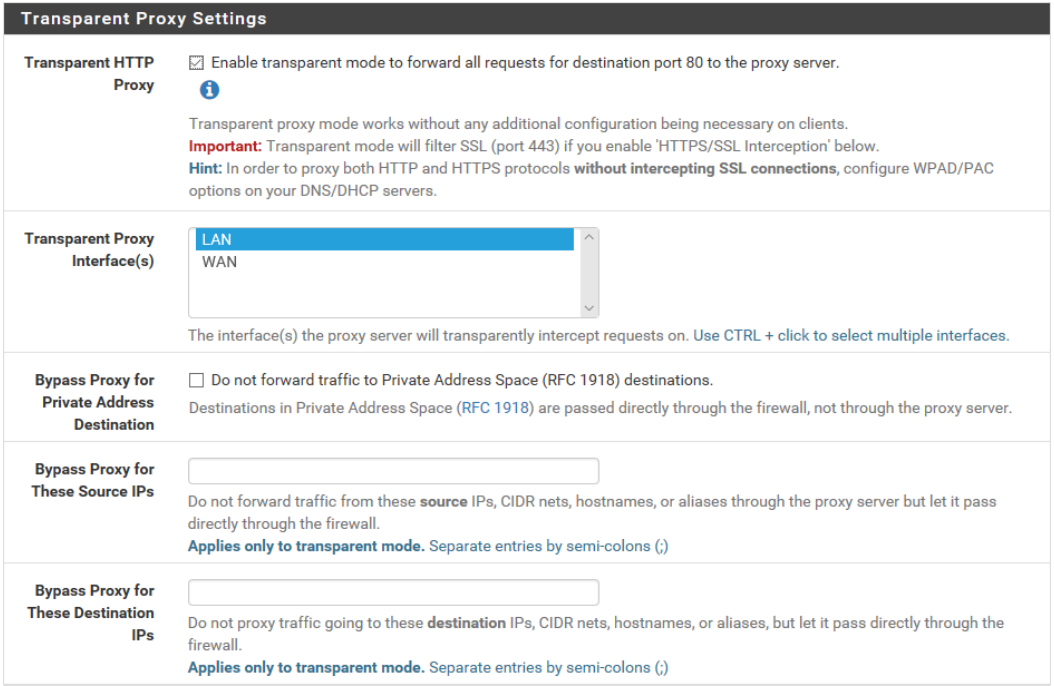
Firewall Implementation

- Firewall appliances
  - Routed (layer 3)
  - Bridged/transparent (layer 2)
  - Router/firewall
- Application-based firewalls
  - Host-based (personal)
  - Application firewall
  - Network operating system (NOS) firewall



Screenshot used with permission from Cisco.

Proxies and Gateways

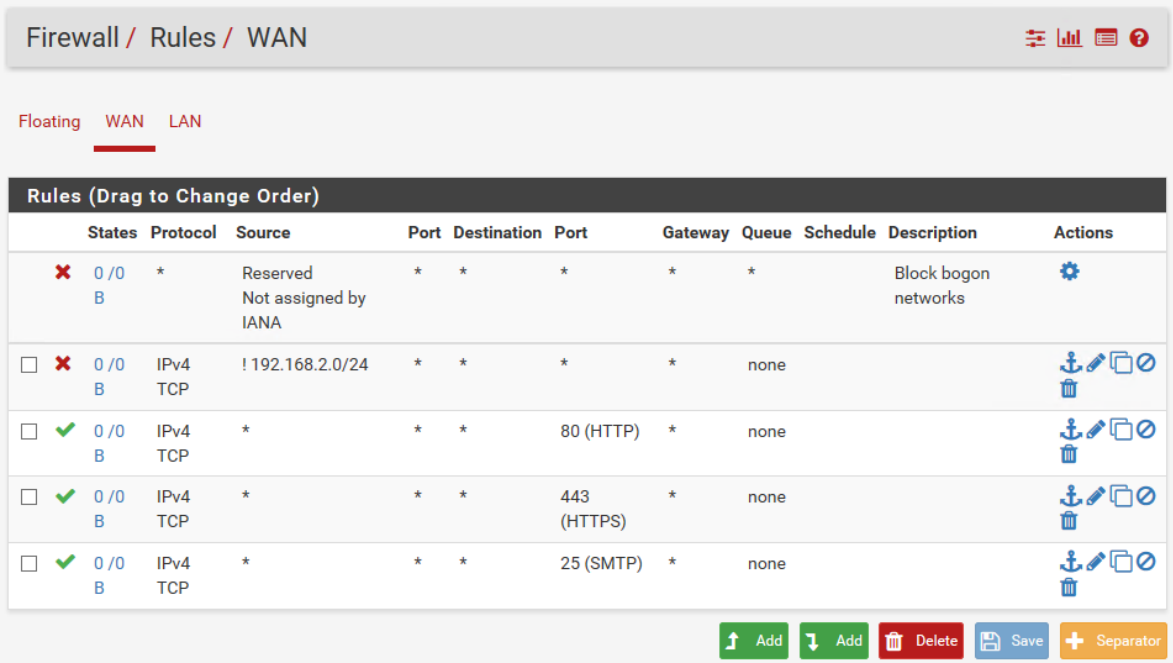


Screenshot used with permission from Rubicon Communications, LLC.

- Forward proxy server
  - Proxy opens connections with external servers on behalf of internal clients
  - Application-specific filters
  - Non-transparent and transparent proxies
  - User authentication
- Reverse proxy server
  - Proxy opens connections with internal servers on behalf of external clients

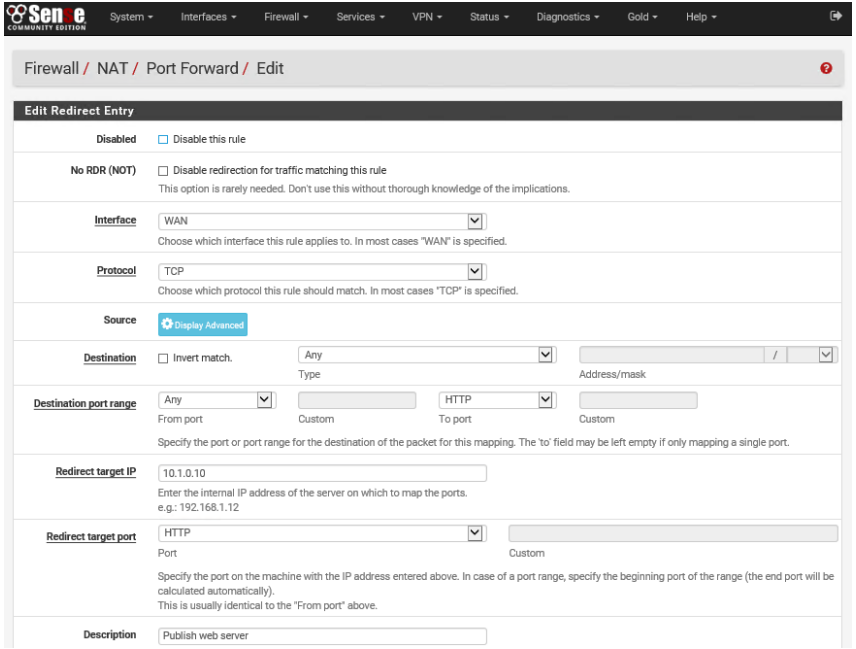
Access Control Lists

- Least access
- Top to bottom processing order
- Implicit deny
- Explicit deny all
- Criteria for rules (tuples)
- Documenting and testing configuration



Screenshot used with permission from Rubicon Communications, LLC.

Network Address Translation



Screenshot used with permission from Rubicon Communications, LLC.

- Source NAT
  - Static and dynamic NAT
  - Overloaded NAT/Network Address Port Translation (NAPT)/Port Address Translation (PAT)
- Destination NAT/port forwarding
  - Advertise a resource using a global IP address but forward it to a local IP address
  - Usually forward specific ports only

Virtual Firewalls

- Hypervisor-based
  - Filtering built into the hypervisor or cloud service
- Virtual appliance
  - Deployed as a virtual machine to the cloud
- Multiple context
  - Firewall appliance running multiple instances
- East-west security design and microsegmentation

Open-source versus Proprietary Firewalls

- Source code inspection and supply chain issues
  - Wholly proprietary appliance OS
  - UNIX or Linux kernel with proprietary features
  - Wholly open-source
- Support arrangements and subscription features

Topic 10B

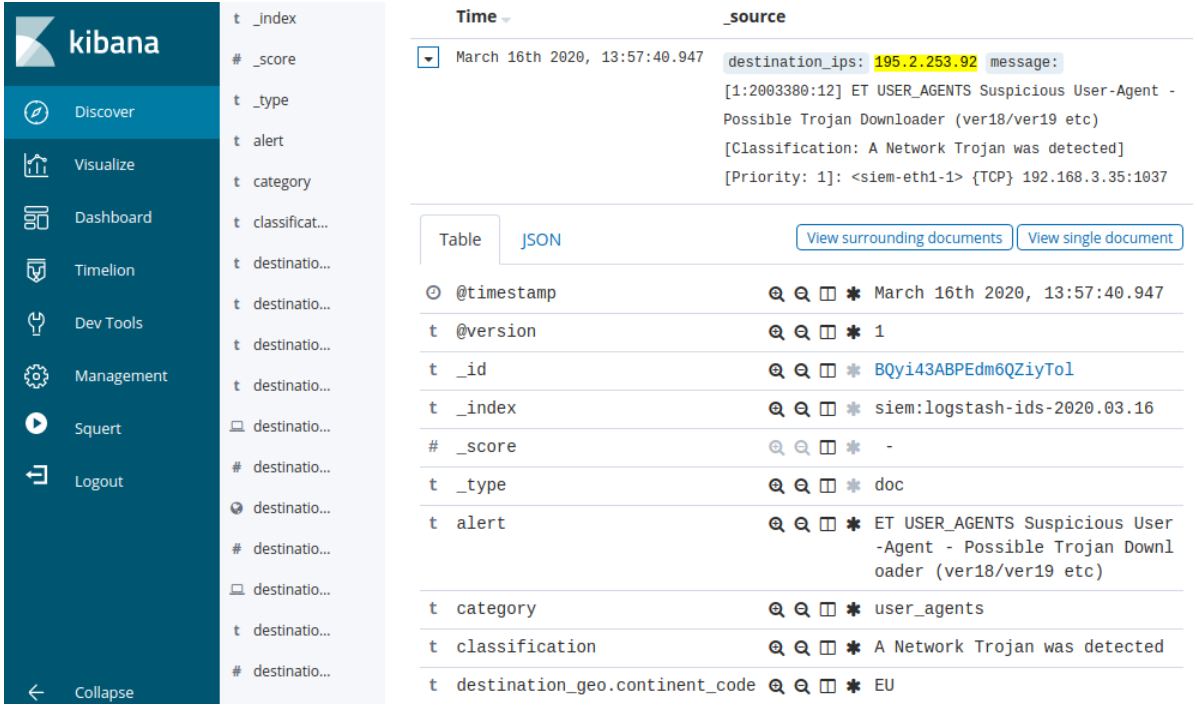
Implement Network Security Monitoring

Syllabus Objectives Covered

- 3.3 Given a scenario, implement secure network designs

Network-Based Intrusion Detection Systems

- Intrusion detection system (IDS)
- Network sensor captures traffic
- Detection engine performs real-time analysis of indicators
- Passive logging/alerting



Screenshot Security Onion securityonion.net

TAPs and Port Mirrors

- Sensor placement
  - Inside firewall
  - In front of application servers
  - Managing volume of traffic/alerts
- Switched port analyzer (SPAN)/mirror port
- Passive test access point (TAP)
- Active TAP
- Aggregation TAP

Network-Based Intrusion Prevention Systems

- Intrusion prevention system (IPS)
- Active response to threats
  - Reset session
  - Apply firewall filters on the fly to shun traffic
  - Bandwidth throttling
  - Packet modification
  - Run a script or other process
- Anti-virus scanning/content filtering
- Inline placement—risk of failure

Signature-Based Detection

```
  GNU nano 2.5.3                    File: downloaded.rules

# ----- Begin ET-emerging-activex Rules Category ----- #

# -- Begin GID:1 Based Rules -- #

#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Internet Explorer Plugin.ocx Heap Overfl$
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX winhlp32 ActiveX control attack - phase 1$
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX winhlp32 ActiveX control attack - phase 2$
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX winhlp32 ActiveX control attack - phase 3$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX MciWndx ActiveX Control"; flow:from_serv$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX COM Object Instantiation Memory Corrupti$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Danim.dll and Dxtmsft.dll COM Objects"; $
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX JuniperSetup Control Buffer Overflow"; f$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Wmm2fxa.dll COM Object Instantiation Mem$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Multimedia Controls - ActiveX $
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Multimedia Controls - ActiveX $
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Multimedia Controls - ActiveX $
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft WMIScriptUtils.WMIObjectBroker$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft VsmIDE.DTE object call CSLID";$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft DExplore.AppObj.8.0 object cal$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft VisualStudio.DTE.8.0 object ca$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Microsoft.DbgClr.DTE.8.0 objec$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft VsaIDE.DTE object call CSLID";$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Business Object Factory object$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Outlook Data Object object cal$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Microsoft Outlook.Application object cal$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX ACTIVEX Possible Microsoft IE Install En$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Possible Microsoft IE Install Engine Ins$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Possible Microsoft IE Shell.Application $
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX ACTIVEX Possible Microsoft IE Shell.Appl$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX NCTAudioFile2 ActiveX SetFormatLikeSampl$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Possible Microsoft Internet Explorer ADO$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Sony ImageStation (SonyISUpload.cab 1.0.$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEX Citrix Presentation Server Client WFICA.$
                              [ Read 27185 lines (Warning: No write permission) ]
```

- Analysis engine
- Signature-based detection
  - Pattern matching
  - Database of known attack signatures
  - Must be updated with latest definitions /plug-ins/feeds
  - Many attack tools do not conform to specific signatures

Behavior and Anomaly-Based Detection

- Behavioral-based detection
  - Train sensor with baseline normal behavior to recognize anomalous behavior
  - Network behavior and anomaly detection (NBAD)
  - Heuristics (learning from experience)
  - Statistical model of behavior
  - Machine learning assisted analysis
    - User and entity behavior analytics (UEBA)
    - Network traffic analysis (NTA)
- Anomaly-based detection as irregularity in packet construction

Next-generation Firewalls and Content Filters

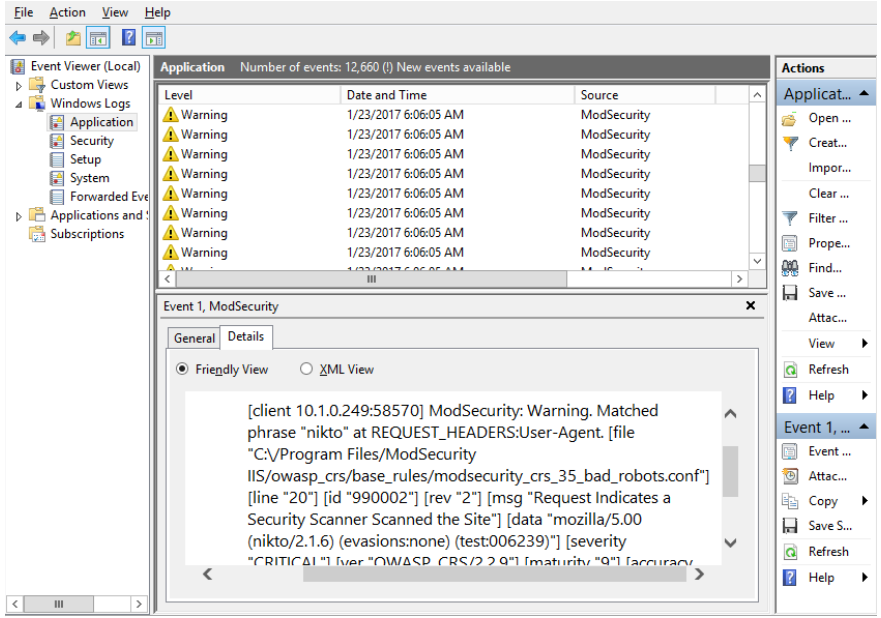
- Next-generation firewall
  - Application-aware filtering, user account-based filtering, IPS, cloud inspection, …
- Unified threat management (UTM)
  - Combining security controls into single agent and management platforms
  - Firewall, anti-malware, network intrusion prevention, spam filtering, content filtering, data loss prevention, VPN, cloud access gateway, …
- Content/URL filter
  - Focuses on outgoing user traffic
  - Content block lists and allow lists
  - Time-based restrictions
  - Secure web gateway (SWG)

Host-Based Intrusion Detection Systems

- Host-based IDS
  - Network, log, and file system monitoring for endpoints
- File integrity monitoring (FIM)
  - Cryptographic hash or file signature verifies integrity of files
  - Compare hashes manually or verify signature with publisher's public key
  - Windows File Protection/sfc
  - Tripwire and OSSEC

Web Application Firewalls

- Able to inspect code in HTTP packets
- Matches suspicious code to vulnerability database
- Can be implemented as software on host or as appliance



Screenshot used with permission from Microsoft.

Topic 10C

Summarize the Use of SIEM

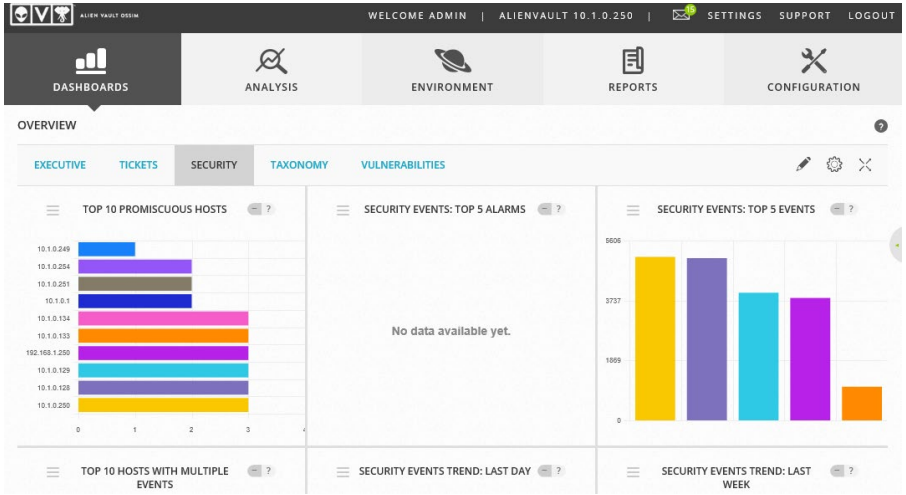
Syllabus Objectives Covered

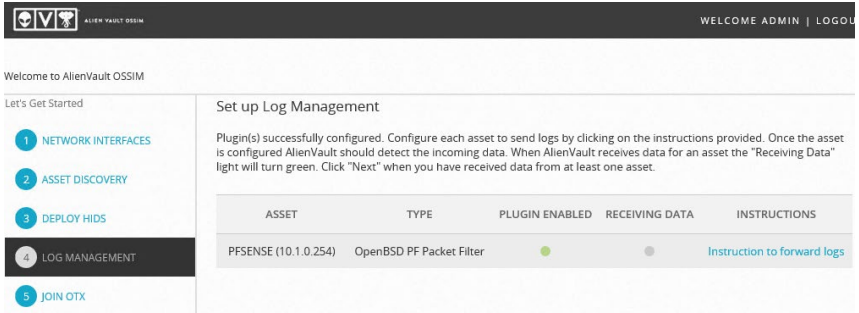
- 1.7 Summarize the techniques used in security assessments
- 3.3 Given a scenario, implement secure network designs
- 4.1 Given a scenario, use the appropriate tool to assess organizational security

Monitoring Services

- Packet capture
  - Sniffers and flow analysis
  - Traffic and protocol statistics
  - Packet analysis
- Network monitors
  - Appliance state data
  - Heartbeat availability monitoring
- Logs
  - System logs to diagnose availability issues
  - Security logs to audit access

Security Information and Event Management





- Log collection
  - Agent-based
    - Local agent to forward logs
  - Listener/collector
    - Protocol-based remote log forwarding (syslog)
  - Sensor
    - Packet capture and traffic flow data
- Log aggregation
  - Consolidation of multiple log formats to facilitate search/query and correlation
  - Normalization of fields
  - Time synchronization

Screenshots used with permission from AT&T Cybersecurity.

Analysis and Report Review

- Correlation
  - Relating security data and threat intelligence
  - Alerting of indicators of compromise (IOC)
  - Basic rules versus machine learning
- User and entity behavior analytics (UEBA)
- Sentiment analysis
  - Machine interpretation of natural language
  - Emotion AI
- Security orchestration, automation, response (SOAR)

File Manipulation

- cat
  - View contents of one or more files
- head and tail
  - View first and last lines of file
- logger
  - Write input to system log

Regular Expressions and grep

- Regular expression syntax
  - Search operators, quantifiers, logic statements, and anchors/boundaries
- grep
  - Searches file contents
  - Simple string matching or regex syntax

```
grep -F 192.168.1.254 access.log
```

```
grep -r 192\.168\.1\.[\d]{1,3}
```

Lesson 10

Summary