

Lesson 10

Implementing Network Security Appliances

Topic 10A

Implement Firewalls and Proxy Servers

Syllabus Objectives Covered

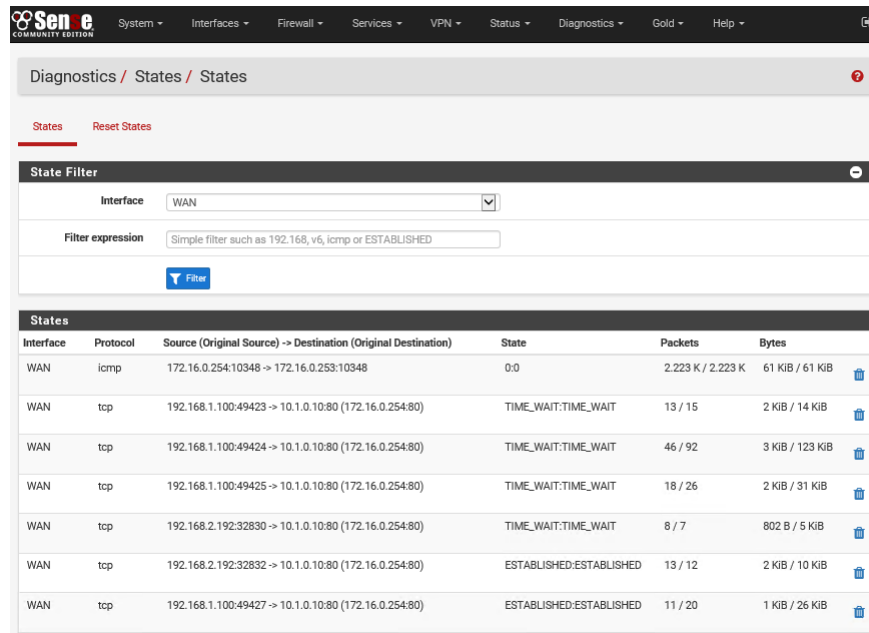
- 3.3 Given a scenario, implement secure network designs

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



The screenshot shows the Mikrotik WinBox interface for the Firewall States page. At the top, there's a navigation bar with 'Diagnostics / States / States'. Below it, there are tabs for 'States' and 'Reset States'. A 'State Filter' section allows filtering by 'Interface' (set to 'WAN') and 'Filter expression' (set to 'Simple filter such as 192.168, v6, icmp or ESTABLISHED'). A 'Filter' button is present. The main table, titled 'States', lists active connections with columns for Interface, Protocol, Source (Original Source) -> Destination (Original Destination), State, Packets, and Bytes. The table contains seven rows of data, showing various ICMP and TCP connections in different states like '0/0', 'TIME_WAIT:TIME_WAIT', and 'ESTABLISHED:ESTABLISHED'.

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

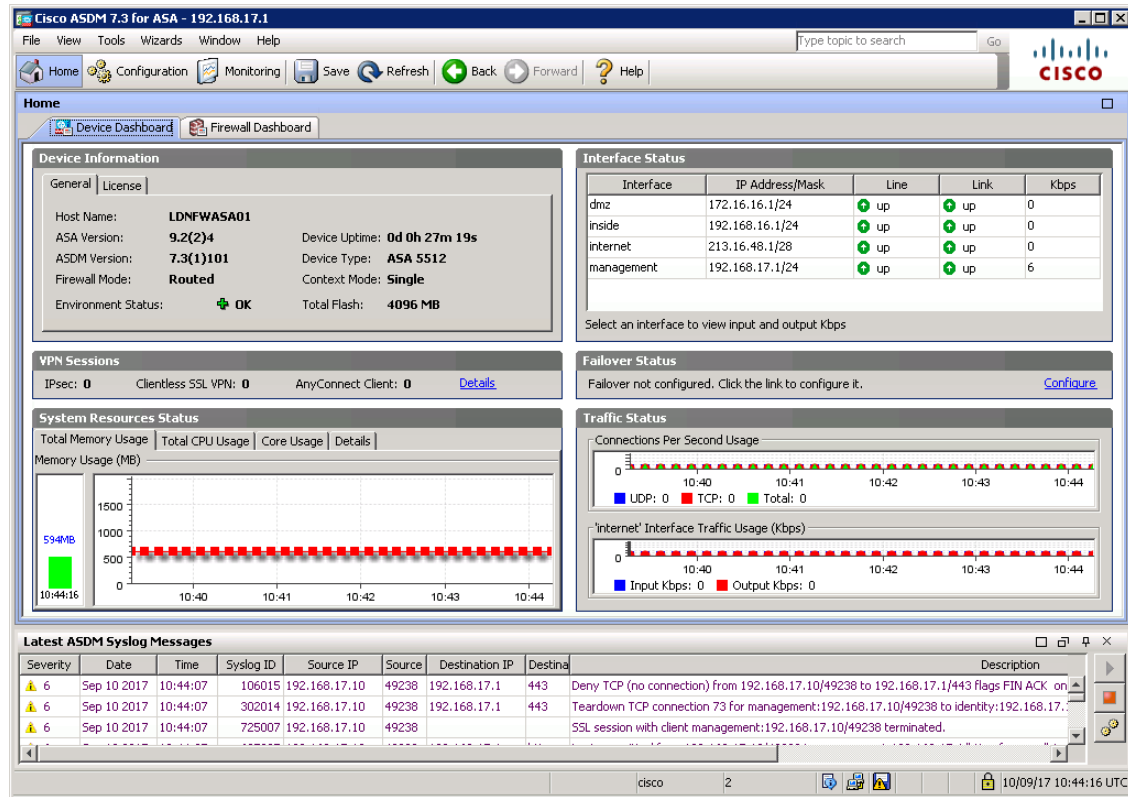
Chain INPUT (policy DROP)

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

Transparent Proxy Settings

Transparent HTTP Proxy

☒ Enable transparent mode to forward all requests for destination port 80 to the proxy server.

Important: Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below.

Hint: In order to proxy both HTTP and HTTPS protocols **without intercepting SSL connections**, configure WPAD/PAC options on your DNS/DHCP servers.

Transparent Proxy Interface(s)

LAN
WAN

The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.

Bypass Proxy for Private Address Destination

☐ Do not forward traffic to Private Address Space (RFC 1918) destinations.

Destinations in Private Address Space (RFC 1918) are passed directly through the firewall, not through the proxy server.

Bypass Proxy for These Source IPs

Do not forward traffic from these **source** IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall.

Applies only to transparent mode. Separate entries by semi-colons (;)

Bypass Proxy for These Destination IPs

Do not proxy traffic going to these **destination** IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall.

Applies only to transparent mode. Separate entries by semi-colons (;)

- 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

Screenshot used with permission from Rubicon Communications, LLC.

Access Control Lists

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

Firewall / Rules / WAN

Floating WAN LAN

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✗ 0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	! 192.168.2.0/24	*	*	*	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	*	*	*	25 (SMTP)	*	none			

Add Add Delete Save Separator

Screenshot used with permission from Rubicon Communications, LLC.

Network Address Translation

Firewall / NAT / Port Forward / Edit

Edit Redirect Entry

Disabled ☒ Disable this rule

No RDR (NOT) ☐ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface: WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

Protocol: TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source: [Display Advanced](#)

Destination: ☐ Invert match. Any / Type: / Address/mask

Destination port range: Any / From port: Custom / HTTP / To port: Custom
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP: 10.1.0.10
Enter the internal IP address of the server on which to map the ports.
e.g.: 192.168.1.12

Redirect target port: HTTP / Port: Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

Description: Publish web server

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

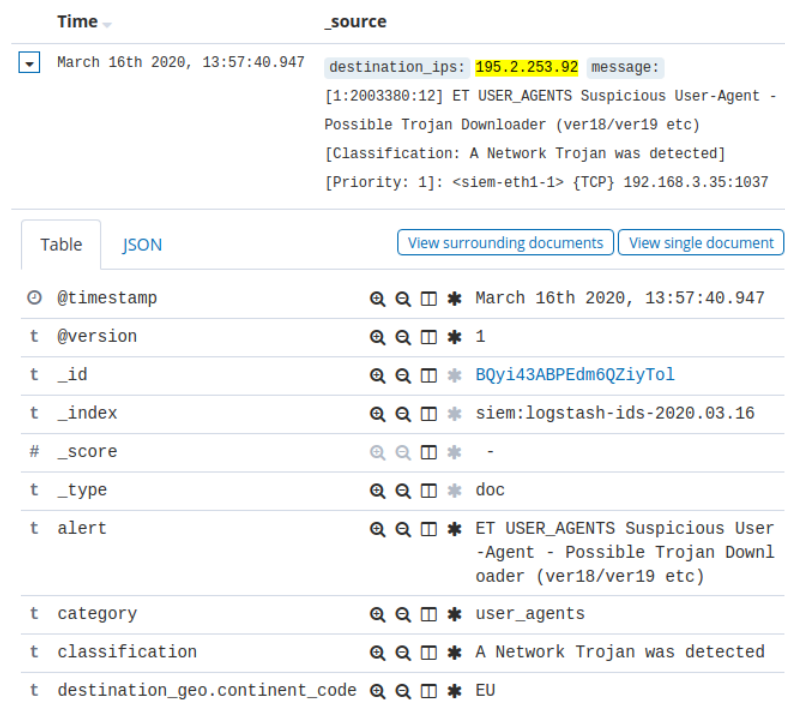
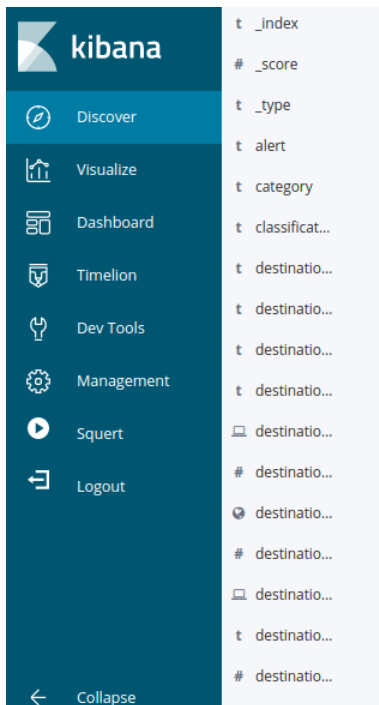
Implement Network Security Monitoring

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 -> $HOME_NET any (msg:"ET ACTIVEV Internet Explorer Plugin.ocx Heap Overfl$
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV winhlp32 ActiveX control attack - phase 1$
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV winhlp32 ActiveX control attack - phase 2$
alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV winhlp32 ActiveX control attack - phase 3$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV MciWndx ActiveX Control"; flow:from_serv$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV COM Object Instantiation Memory Corrupti$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Danim.dll and Dxtmsft.dll COM Objects"; $
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV JuniperSetup Control Buffer Overflow"; f$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Wmm2fxa.dll COM Object Instantiation Mem$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Microsoft Multimedia Controls - ActiveX $
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Microsoft Multimedia Controls - ActiveX $
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Microsoft Multimedia Controls - ActiveX $
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Microsoft WMIScriptUtils.WMIObjectBroker$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Microsoft VsmIDE.DTE object call CSLID";$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Microsoft DExplore.AppObj.8.0 object cal$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Microsoft VisualStudio.DTE.8.0 object ca$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Microsoft Microsoft.DbgClr.DTE.8.0 objec$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Microsoft VsaIDE.DTE object call CSLID";$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Microsoft Business Object Factory object$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Microsoft Outlook Data Object object cal$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Microsoft Outlook.Application object cal$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV ACTIVEX Possible Microsoft IE Install En$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Possible Microsoft IE Install Engine Ins$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Possible Microsoft IE Shell.Application $
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV ACTIVEX Possible Microsoft IE Shell.Appl$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV NCTAudioFile2 ActiveX SetFormatLikeSampl$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Possible Microsoft Internet Explorer ADOS$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Sony ImageStation (SonyISUpload.cab 1.0.$
#alert tcp $EXTERNAL_NET $HTTP_PORTS -> $HOME_NET any (msg:"ET ACTIVEV Citrix Presentation Server Client WFICA.$

[ 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

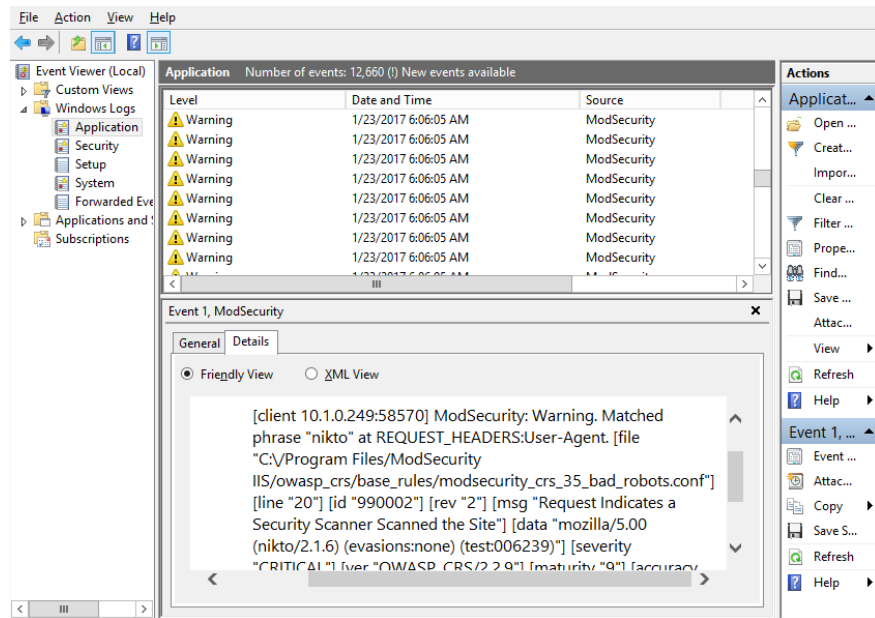
- Next-generation firewall
 - Application-aware filtering, user account-based filtering, IPS, cloud inspection, ...
- Unified threat management (UTM)
 - Combining security controls into single agent and management platforms
 - Firewall, anti-malware, network intrusion prevention, spam filtering, content 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

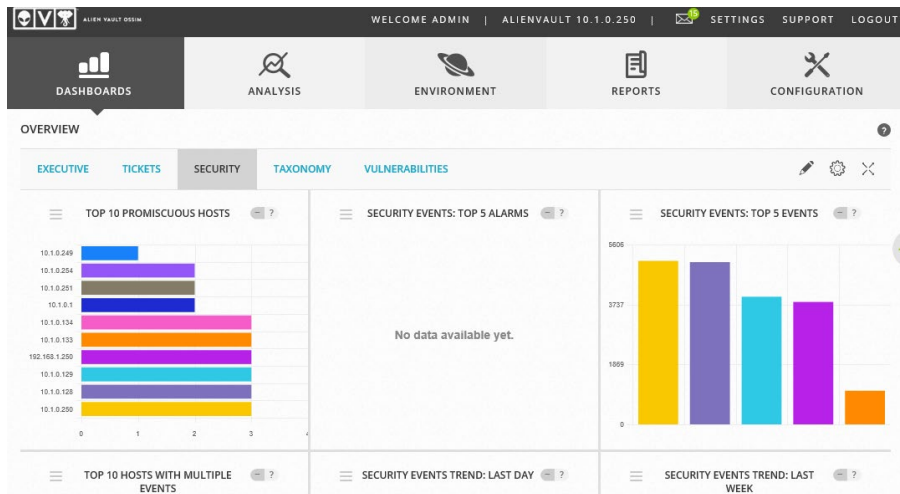
Syllabus Objectives Covered

- 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

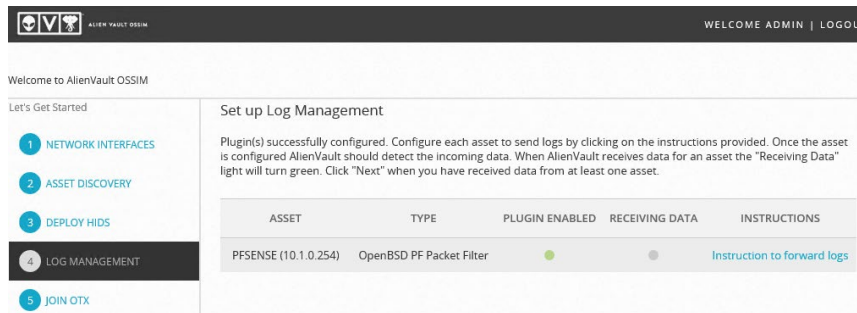
Monitoring Services

- 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



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

