

Nicholas Marshall

Dr. Nelbert St. Clair

ITEC 4345 – Cyber Systems Security

February 28, 2019

Palo Alto Networks Lab 5

3. Create Security Policy Rule With an Antivirus Profile:

The screenshot shows the Palo Alto Networks Security Policy Rule configuration interface. The left sidebar displays a tree view of the configuration hierarchy, including Security, NAT, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, and DoS Protection. The main pane shows a table of security rules. The rule 'egress-outside-av' is selected, and its configuration is displayed in the right pane. The rule is configured with the following settings:

Name	Tags	Type	Zone	Address	User	HTTP Profile	Zone	Address	Application	Service
1 egress-outside-av	egress	universal	any	any	any	any	any	any	any	application
2 egress-outside-app-id	egress	universal	any	any	any	any	any	any	any	application
3 egress-outside	egress	universal	any	any	any	any	any	any	any	application
4 internal-dmz-ftp	internal	universal	any	any	any	any	any	any	any	application
5 intrazone-default	none	intrazone	any	any	any	any	any	any	any	any
6 interzone-default	none	interzone	any	any	any	any	any	any	any	any

The rule is configured with the following settings:

- Name: egress-outside-av
- Tags: egress
- Type: universal
- Zone: any
- Address: any
- User: any
- HTTP Profile: any
- Zone: any
- Address: any
- Application: any
- Service: application

The rule is configured with the following settings:

- Name: egress-outside-av
- Tags: egress
- Type: universal
- Zone: any
- Address: any
- User: any
- HTTP Profile: any
- Zone: any
- Address: any
- Application: any
- Service: application

4. Test Security Policy Rule:

The screenshot shows a web browser window displaying a message from Eicar, indicating that the download of a virus/spyware file has been blocked. The message reads:

Virus/Spyware Download Blocked

Download of the virus/spyware has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

File name: eicar.com.txt

The browser address bar shows the URL: 2016.eicar.org/download/eicar.com.txt. The browser window is titled "Eicar - EUROPEAN EXPERIMENTAL INSTITUTE FOR CYBERSECURITY".

5. Review Logs:

PAN8_210_Master_Client - VMware Workstation

File Edit View VM Tabs Help

Library

My Computer

- Windows 7
- Kali
- Windows Server 2016
- Windows XP Professional
- Helix
- Ubuntu/VM-NCM
- Windows Server 2016
- ESXi6-NCM
- Palo Alto Networks Lab
 - PAN8_210_Master_FW
 - PAN8_210_Master_Client
 - PAN8_210_Master_VR
 - PAN8_210_Master_DMZ
- Shared VMs

Home | PAN8_210_Master_Client | PAN8_210_Master_VR | PAN8_210_Master_DMZ | Palo Alto Networks Lab | PAN8_210_Master_FW

lab-firewall

https://192.168.1.254/#monitorcvsys1:monitor/logs/threat

paloalto NETWORKS

Dashboard ACC Monitor Policies Objects Network Device

Commit Config Search

Manual

Logs

- Traffic
- Threat
- URL Filtering
- WildFire Submissi
- Data Filtering
- HIP Match
- User-ID
- Tunnel Inspection
- Configuration
- System
- Alarms
- Authentication
- Unified
- Packet Capture
- App Scope
- Summary
- Change Monitor
- Threat Monitor
- Network Map
- Traffic Map
- Session Browser
- Botnet
- PDF Reports
- Manage PDF Sumr
- User Activity Repc

Packet Capture

02/28 23:43:23:43:15.000000

0x0020: c63a d349 0050 1184 6aa3 88b3 37d5 5018 .I.P..J...7.P.

0x0030: f4f8 0000 0000 332e 3135 3531 3339 37333.15513973

0x0040: 3d33 2e30 005f 706b 5f73 6573 2631 2663 63.j..pk_sas.1.c

0x0050: 3262 613d 310d 000d 0a 20a1....

0x0060: 000c 2902 3c3a 000c 2972 c6d3 0000 4500 ..I..J...E.

0x0070: 0180 9562 0000 7f0e 473e d5d3 c63a c80a ...b...G.....

0x0080: 0114 0050 d349 88b3 37d5 1184 6a0c 5018 ...P.I..7...J.P.

0x0090: f4f8 002e 0000 4854 5450 2f31 2e31 2832HTTP/1.1.2

0x00a0: 3030 204f 0000 0a44 6174 653a 2054 6875 00.Ok..Date:Thu

0x00b0: 2c20 3238 2046 6562 2032 3031 3920 3233 ,,28.Feb.2019.23

0x00c0: 3a3a 333a 3231 2047 4d5a 000a 5305 727e :43:21 GMT..Serv

0x00d0: 6572 3a20 4170 6163 6865 2f32 2e34 2e31 er:Apache/2.4.1

0x00e0: 3020 2844 6562 6961 6a29 000a 436f 6e7a 0.(Debian)..Cont

0x00f0: 656e 742d 6409 7370 6f73 69f4 6e6f 6e3a ent-disposition:

0x0100: 2061 7474 6163 686d 656e 743b 2066 696c .attachment;fil

0x0110: 656e 616d 653d 2265 6963 6172 2e63 6f6d ename="eicar.com

0x0120: 2e74 7874 2200 0a43 6163 6865 2e63 6f6e .txt"..cache-con

0x0130: 7472 6f6c 3a20 7072 6976 6174 650d 0a43 trol:private..C

0x0140: 6f6e 7465 6e74 206c 656e 6774 683a 2036 ontent-Length:6

0x0150: 300d 0a4b 6565 702d 416c 6976 653a 2074 0..keep-Alive:t

0x0160: 696d 656f 7574 3035 2c20 6d61 783d 3130 imeout=5,max=10

0x0170: 300d 0a43 6f6e 6e65 6374 696f 6e3a 204b 0..Connection:K

0x0180: 6565 702d 416c 6976 650d 0a43 6f6e 7465 eep-Alive.Conte

0x0190: 6e74 2e54 7970 653a 0b61 7070 6c09 6361 nt-Type: application

0x01a0: 7469 6f6e 2f6f 6374 6574 2d73 7472 6561 tion/octet-strea

0x01b0: 6d0d 0a0d 0a5d 354f 2150 2540 4150 5034 m...ISO/Pgmp[4

0x01c0: 5150 5a58 3534 2050 5a29 3743 4129 377d VZXA4(P7CC)7

0x01d0: 2445 4943 4152 2053 5441 4e44 4152 4a2d SEICAR-STANDARD

0x01e0: 4150 5a49 656d 5255 5102 6445 5354 2046 ANTIVIRUS-TEST-P

0x01f0: 494c 4531 2049 704b 700b 0a 11111111..

Export Close

admin | Logout | Last Login Time: 02/28/2019 22:51:04

Displaying logs 1-1 | 20 | per page | DESC

Tasks | Language

Standard build 9600

11:45 PM

2/28/2019

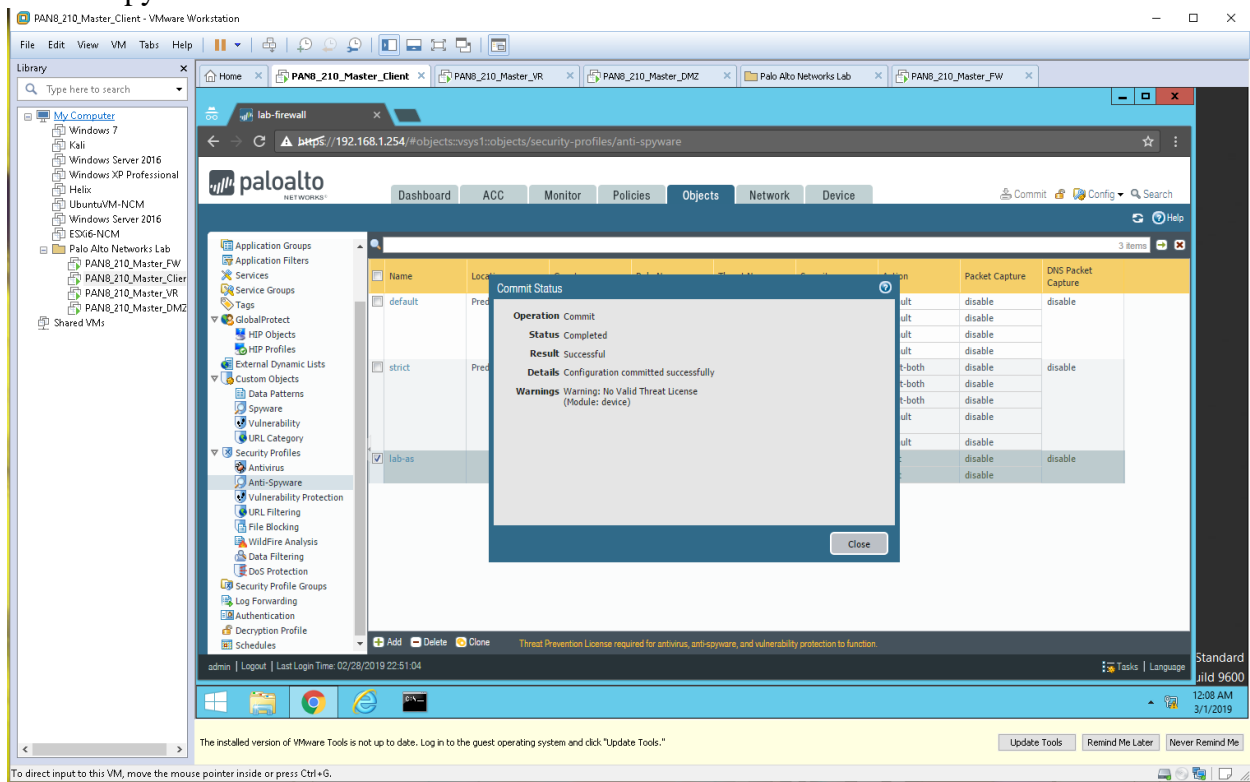
The installed version of VMware Tools is not up to date. Log in to the guest operating system and click "Update Tools."

Update Tools | Remind Me Later | Never Remind Me

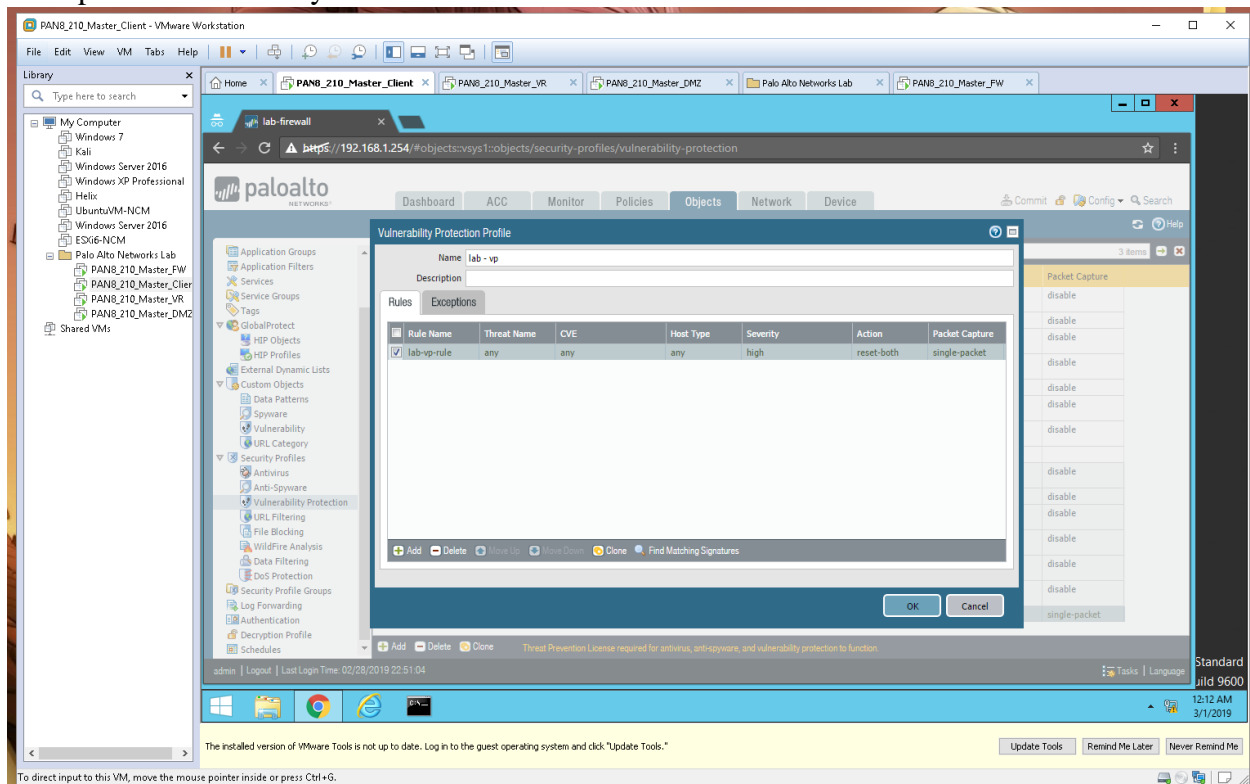
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

[illegible]

9. Anti-Spyware Profile with DNS Sinkhole:



15. Update Vulnerability Profile:



18. Modify Security Profile Group:

The screenshot shows the Palo Alto Networks GUI within a VMware Workstation environment. The left sidebar displays the 'Library' tree with the 'Palo Alto Networks Lab' expanded, showing various objects including 'Security Profile Groups'. The main pane shows the 'Security Profile Groups' configuration page for the 'lab-spg' group. The page includes a table with columns for Name, Location, Antivirus Profile, Anti-Spyware Profile, Vulnerability Protection Profile, URL Filtering Profile, File Blocking Profile, Data Filtering Profile, and WildFire Analysis Profile. The 'lab-spg' group is listed with the following profiles:

Name	Location	Antivirus Profile	Anti-Spyware Profile	Vulnerability Protection Profile	URL Filtering Profile	File Blocking Profile	Data Filtering Profile	WildFire Analysis Profile
lab-spg		lab-av	lab-as	lab-vp		lab-file-blocking		

The bottom status bar indicates the installed version of VMware Tools is not up to date and provides a link to 'Update Tools'.