

SIDDHANT GAHTORI

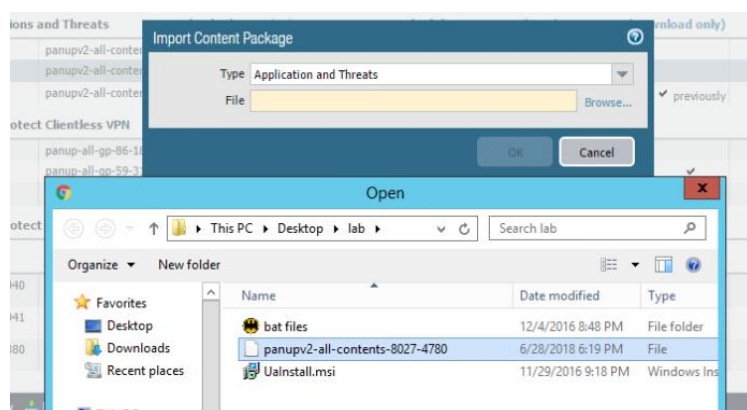
ESSENTIAL PROJECT II

Module 1A (LAB 8): Securing Endpoints

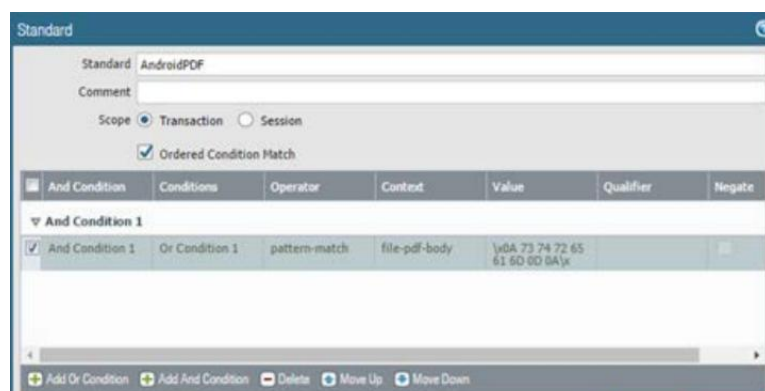
Summary: In this module, we tried and tested different methods to secure endpoints. We can do this by simply updating antivirus of the device and we can also upload custom AV to palo alto firewall. We can also create Vulnerability Signature.

Version	File Name	Features	Type	Size	Release Date	Downloaded	Currently Installed	Action	Documentation
▼ Antivirus Last checked: 2020/05/06 09:32:14 UTC Schedule: None									
2113-2598	panup-all-antivirus-2113-2598		Full	67 MB	2017/01/03 21:51:36 UTC	✓ previously		Revert	Release Notes
2141-2627	panup-all-antivirus-2141-2627		Full	67 MB	2017/01/31 21:45:52 UTC	✓	✓		Release Notes
3339-3850	panup-all-antivirus-3339-3850		Full	103 MB	2020/05/05 11:02:55 UTC			Download	Release Notes
▼ Applications and Threats Last checked: 2020/05/06 09:32:13 UTC Schedule: Every Wednesday at 01:02 (Download only)									

◆ Antivirus Update



◆ Custom Antivirus Check



◆ Creating Vulnerability Signature

Module 1B (LAB 9): Stopping Reconnaissance Attacks

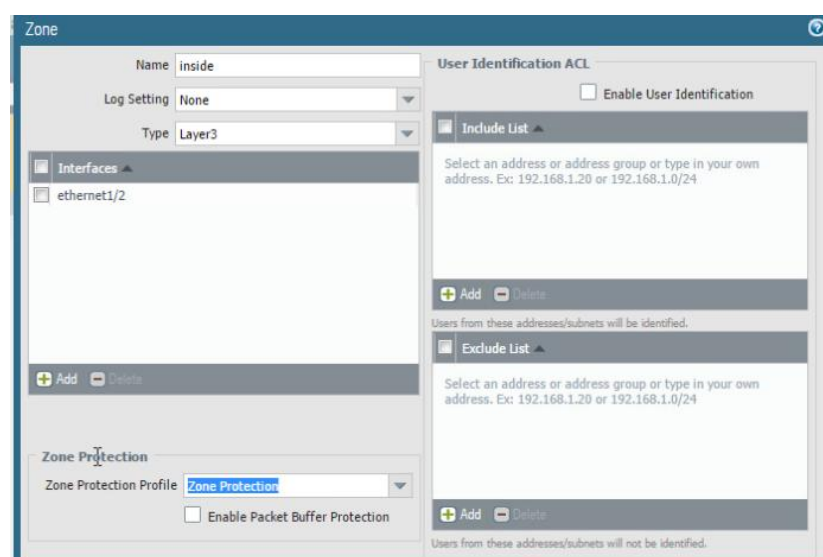
Summary: In this lab, first we made zone protection profile then applied it to all 3 zones (inside, outside, dmz). We enabled flood & reconnaissance protection. After that we tested it with the help of Zenmap and analyzed the results.



The screenshot shows the 'Zone Protection Profile' configuration window. The 'Name' field is 'Zone Protection' and the 'Description' is 'Protect against NMAP Scan'. There are four tabs: 'Flood Protection', 'Reconnaissance Protection', 'Packet Based Attack Protection', and 'Protocol Protection'. The 'Reconnaissance Protection' tab is active, showing a table with the following data:

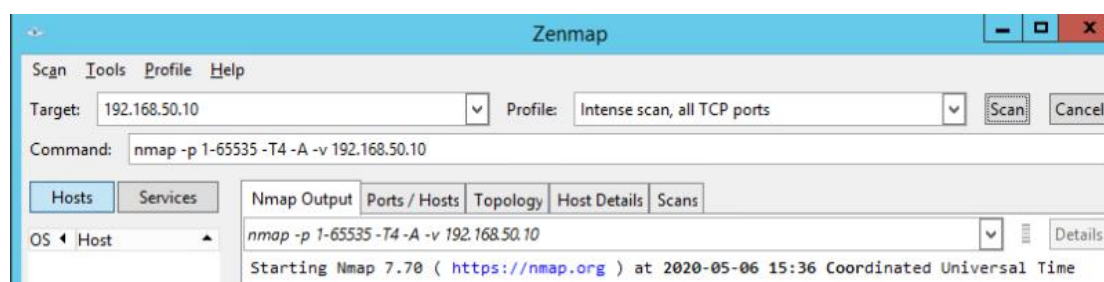
Scan	Enable	Action	Interval (sec)	Threshold (events)
TCP Port Scan	<input checked="" type="checkbox"/>	block	10	40
Host Sweep	<input checked="" type="checkbox"/>	block	10	40
UDP Port Scan	<input checked="" type="checkbox"/>	block	10	40

◆ Zone Protection Profile Configuration



The screenshot shows the 'Zone' configuration window. The 'Name' field is 'inside', 'Log Setting' is 'None', and 'Type' is 'Layer3'. The 'Interfaces' list contains 'ethernet1/2'. The 'Zone Protection' section shows 'Zone Protection Profile' set to 'Zone Protection' and 'Enable Packet Buffer Protection' is unchecked. The 'User Identification ACL' section has 'Enable User Identification' unchecked, with empty 'Include List' and 'Exclude List' fields.

◆ Applying Zone Protection to all the Zones



The screenshot shows the Zenmap interface. The 'Target' field is '192.168.50.10' and the 'Profile' is 'Intense scan, all TCP ports'. The 'Command' field contains 'nmap -p 1-65535 -T4 -A -v 192.168.50.10'. The 'Nmap Output' tab is active, showing the command 'nmap -p 1-65535 -T4 -A -v 192.168.50.10' and the status 'Starting Nmap 7.70 (https://nmap.org) at 2020-05-06 15:36 Coordinated Universal Time'.

◆ Testing With Zenmap

DashboardACCMonitorPoliciesObjectsNetworkDevice

Commit

Config

Search

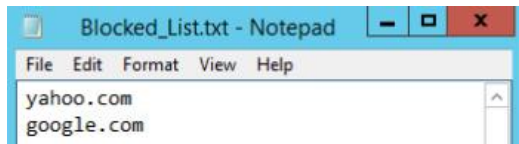
Manual

Help

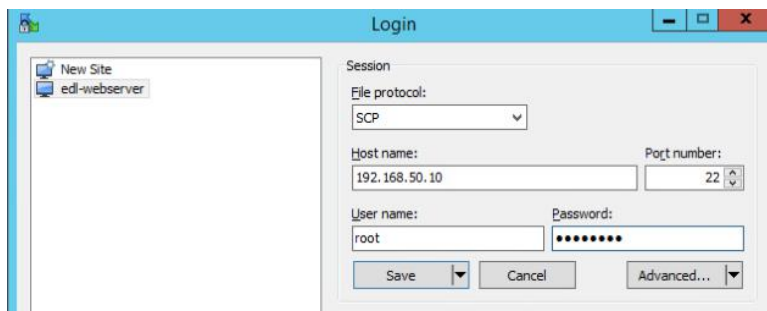
◆ Firewall has blocked the action (Testing Successful)

Module 2A (LAB 10): Using Dynamic Block List

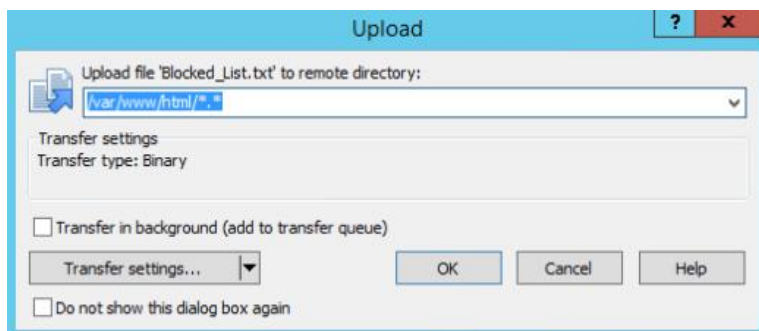
Summary: In this module, we made a custom block list and applied it to our firewall to block certain type of web URLs.



- ◆ List of websites you want to block



- ◆ Changing login credentials for server



- ◆ Uploading the block list

		distribution, command-and-control, or for launching various attacks				
<input checked="" type="checkbox"/>	block-list			http://192.168.50.10/block-list.txt	None	Five Minute

- ◆ Creating a block list inside the firewall

Source												
			Source				Destination					
Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	P
1 Block-List	none	universal	any inside	any	any	any	any outside	any	any	application-default	Deny	n
2 Allow Inside Out	any	universal	any inside	any	any	any	any outside	any	any	application-default	Allow	n

- ◆ Creation of a security policy for block list

Module 3A (LAB 11): Denying International Attackers

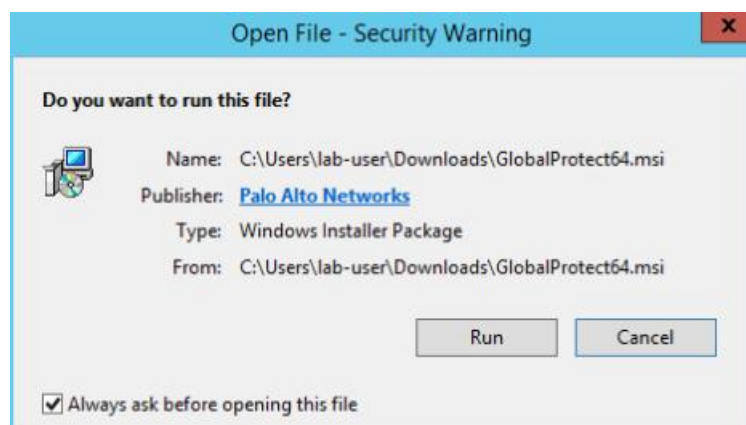
Summary: In this module, we blocked traffic originating from China, KP(North Korea) and Russia to block international attackers to access our internal network data. This was done by changing the security policy.

	Name	Tags	Type	Source				Destination		Application	Service	Action	Pr
				Zone	Address	User	HIP Profile	Zone	Address				
1	Block-Countries	none	universal	outside	CN KP RU	any	any	outside	any	any	application-default	Deny	

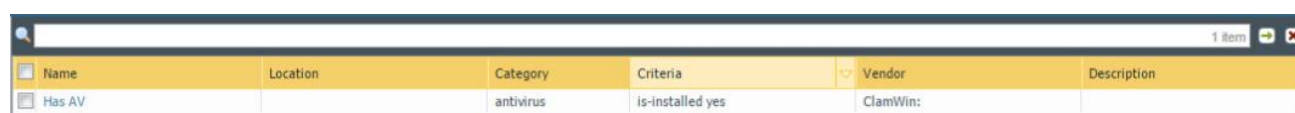
◆ Security Policy Configuration

Module 3B (LAB 12): Configuring HIP for Global Protect

Summary: In this lab, we downloaded and installed GlobalProtect™ while utilizing a HIP Object within a HIP Profile. ClamWin antivirus software was also used within the HIP Profile to configure GlobalProtect to only connect when ClamWin is installed.

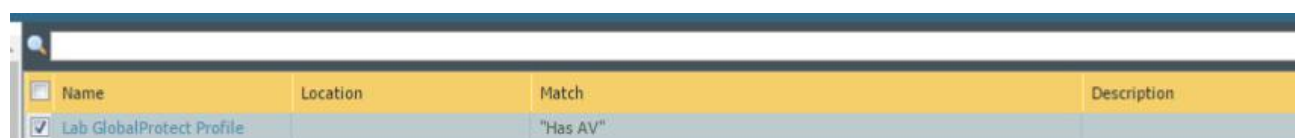


◆ Installation of Global Protect



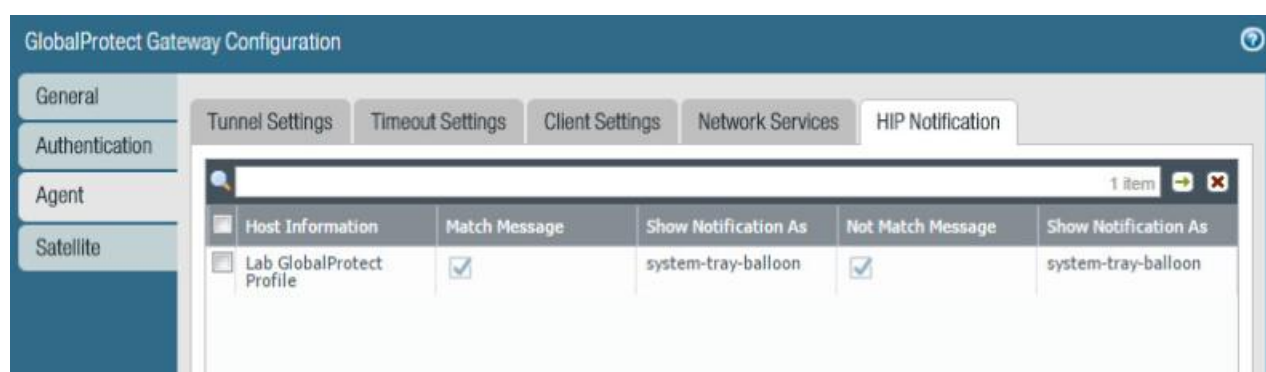
Name	Location	Category	Criteria	Vendor	Description
Has AV		antivirus	is-installed yes	ClamWin:	

◆ HIP user configuration

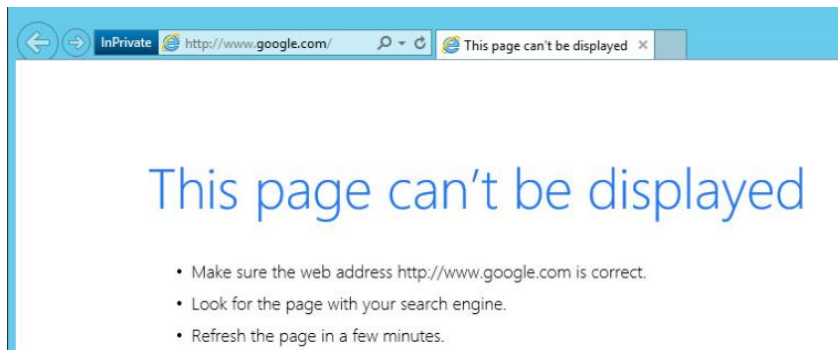


Name	Location	Match	Description
Lab GlobalProtect Profile		"Has AV"	

◆ HIP Profile Creation



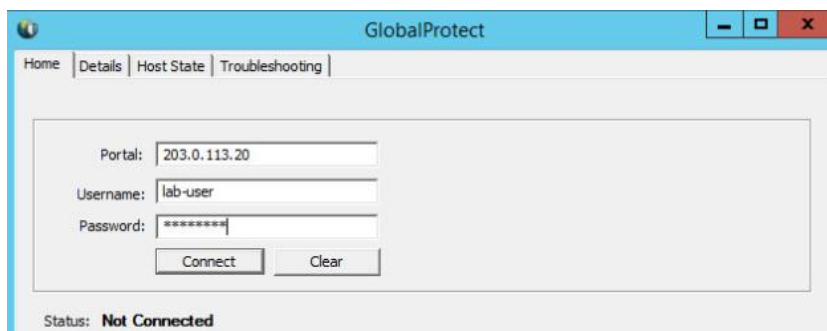
◆ Gateway Configuration for Global Connect



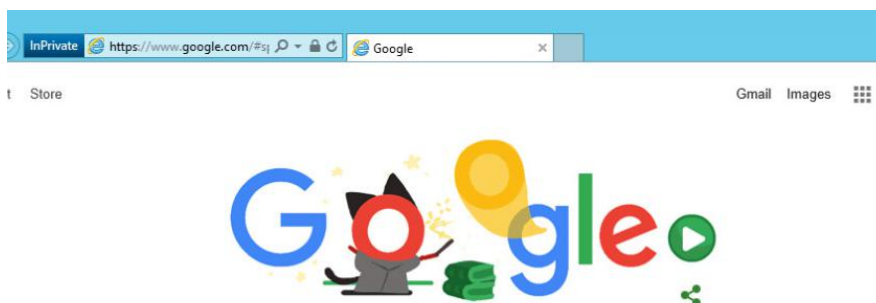
◆ No Internet Access without ClaimWin Antivirus



◆ ClaimWin Downloaded & Installed



◆ Global Protect Connecting





◆ Now you can Access Internet

Project Introduction:

In this project, you will perform the following tasks:

1. Create a Decryption Policy
2. Create a SSH session with Putty and verify Decryption is working.
3. Disable Decryption Policy and show SSH traffic is not being Decrypted.

Screenshots:

	Name	Tags	Source			Destination		URL Category	Service	Action
			Zone	Address	User	Zone	Address			
1	Decrypting SSH	none	 inside	any	any	 dmz	any	any	any	decrypt

◆ Creation of the Policy

Dashboard
ACC
Monitor
Policies
Objects
Network
Device

☒ Receive Time
☒ Decrypted
☒ Type
☒ From Zone
☒ To Zone
☒ Source
☒ Source User

	Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Decrypted
	05/06 02:06:59	end	inside	dmz	192.168.1.20		192.168.50.10	22	ssh	Columns

- ◆ Decrypting traffic in logs

-THE END-