

Team B:  
Grant Arnold  
Mehmett Ozman  
Jackson Pence  
Andre Davis

## PANFW-1 Screenshots:

### NAT Rules Pt.1

The screenshot shows the Palo Alto Networks PAN-OS web interface. The title bar indicates it's running on a VM named '4777B05Honey on SECNET'. The URL in the address bar is <https://192.168.74.113/#policies:vsys1:policies/nat-rulebase>. The navigation bar includes tabs for Dashboard, ACC, Monitor, Policies (which is selected), Objects, Network, Device, Commit, Config, and Search.

The left sidebar menu is expanded to show the NAT section under Security. Other sections like Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection, and SD-WAN are also listed. A 'Policy Optimizer' section is visible, showing rule usage statistics: 'Unused in 30 days' (1), 'Unused in 90 days' (1), and 'Unused' (1).

The main content area displays a table titled 'Original Packet' containing three NAT rules:

	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Se
1	Internet NAT	none	inside	outside	ethernet1/1	any	any	an
2	DMZ To Public	none	dmz	outside	ethernet1/1	any	any	an
3	NAT Private to Public	none	inside	outside	ethernet1/2	any	any	an

At the bottom of the interface, there are buttons for Add, Delete, Clone, Enable, Disable, Move, PDF/CSV, Highlight Unused Rules, Reset Rule Hit Counter, Group, View Rulebase as Group, and a user status message: 'admin | Logout | Last Login Time: 02/01/2022 20:33:14'.

Team B:  
Grant Arnold  
Mehmett Ozman  
Jackson Pence  
Andre Davis

## NAT Rules Pt.2: (Shows Hit Count)

The screenshot shows the Palo Alto Networks Management Console interface. The title bar indicates the connection is to a virtual machine named '4777BPAFW01'. The main navigation bar includes File, Action, Media, Clipboard, View, Help, and tabs for Dashboard, ACC, Monitor, Policies (which is selected), Objects, Network, Device, Commit, Config, and Search.

The left sidebar menu lists various security features: Security, NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection, and SD-WAN. A 'Policy Optimizer' section is also present, showing 'Rule Usage' statistics: 1 Unused in 30 days, 1 Unused in 90 days, and 1 Unused.

The central content area is titled 'Rule Usage' with the sub-instruction: 'Monitoring rule usage can help ensure rules are performing as expected, and can help identify rules that should be removed to reduce your attack surface.' It includes filters for Timeframe (All time), Usage (Any), and Exclude rules reset during the last 90 days. A table titled 'Rule Usage' displays three entries:

Name	Hit Count	Last Hit	First Hit	Reset Date	Modified	Created
Internet NAT	716	2022-02-01 20:35:27	2022-02-01 18:54:46	-	2022-02-01 18:54:49	2022-02-01 18:54:49
DMZ To Public	756	2022-02-01 20:35:27	2022-02-01 18:54:46	-	2022-02-01 18:54:49	2022-02-01 18:54:49
NAT Private to Public	0	-	-	-	2022-02-01 18:54:49	2022-02-01 18:54:49

At the bottom, there are links for Object: Addresses, PDF/CSV, and Reset Rule Hit Counter. The footer shows the user is 'admin' and last logged in at '02/01/2022 20:33:14'. Navigation icons for mail, tasks, and language selection are also present.

Team B:  
Grant Arnold  
Mehmett Ozman  
Jackson Pence  
Andre Davis

## Security Rules: Pt. 1

The screenshot shows the Palo Alto Networks Management Console interface. The top navigation bar includes File, Action, Media, Clipboard, View, Help, and tabs for Dashboard, ACC, Monitor, Policies (selected), Objects, Network, Device, Commit, Config, and Search. The left sidebar under the Security category lists NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection, and SD-WAN. The main content area displays the security rulebase table with the following data:

Name	Tags	Type	Source					Zone
			Zone	Address	User	HIP Profile		
Internet NAT	none	universal	inside	any	any	any	outside	
DMZ-NAT	none	universal	dmz	any	any	any	outside	
intrazone-default	none	intrazone	any	any	any	any	(intrazone)	
interzone-default	none	interzone	any	any	any	any	any	

Below the table, the Policy Optimizer section shows:

- No App Specified: 2
- Unused Apps: 0
- Rule Usage
  - Unused in 30 days: 0
  - Unused in 90 days: 0
  - Unused: 0

At the bottom, the Object: Addresses pane shows standard network management controls like Add, Delete, Clone, Override, Revert, Enable, Disable, Move, PDF/CSV, Highlight Unused Rules, Reset Rule Hit Counter, Group, Logout, Tasks, and Language.

Team B:  
Grant Arnold  
Mehmett Ozman  
Jackson Pence  
Andre Davis

## Security Policies (Hit Count)

The screenshot shows the Palo Alto Networks UI interface. The top navigation bar includes File, Action, Media, Clipboard, View, Help, and tabs for Dashboard, ACC, Monitor, Policies (which is selected), Objects, Network, and Device. Below the navigation is a toolbar with icons for file operations like Open, Save, Print, and a search bar. The main content area displays a table titled "Security Policies (Hit Count)" with the following data:

Application	Service	Action	Profile	Options	Hit Count	Last Hit
any	application-d...	Allow	none	edit icon	1091	2022-02-01 20:34:46
any	application-d...	Allow	none	edit icon	1131	2022-02-01 20:34:46
any	any	Allow	none	edit icon	925	2022-02-01 20:33:05
any	any	Deny	none	edit icon	480	2022-02-01 18:54:36

On the left sidebar, under the "Security" section, there are links for NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection, and SD-WAN. A "Policy Optimizer" section shows metrics for No App Specified (2), Unused Apps (0), and Rule Usage (Unused in 30 days: 0, Unused in 90 days: 0, Unused: 0). At the bottom, there is an "Object : Addresses" list and a toolbar with buttons for Add, Delete, Clone, Override, Revert, Enable, Disable, Move, PDF/CSV, Highlight Unused Rules, Reset Rule Hit Counter, and Group.

Team B:  
Grant Arnold  
Mehmett Ozman  
Jackson Pence  
Andre Davis

## **FIREWALL 2: 4777PANFWB02:**

### **NAT Policies For Second Firewall:**

The screenshot shows the Palo Alto Networks Firewall 2 interface. The title bar indicates it's connected to a pfSense home.arpa - Diagnostic VM. The browser address bar shows the URL <https://192.168.74.114/#policies:vsys1:policies/nat-rulebase>. The main window displays the 'NAT' section under the 'Security' category. It lists four NAT rules:

Rule	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Action
1	Internet NAT	none	inside	outside	ethernet1/1	any	any	an
2	DMZ-NAT	none	dmz	outside	any	any	any	an
3	NAT Private To Public	none	inside	outside	ethernet1/2	any	any	an
4	egress-outside	egress	inside	outside	ethernet1/1	any	any	an

The left sidebar also shows other security categories like Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection, and SD-WAN. A 'Policy Optimizer' section is visible, showing rule usage statistics. The bottom navigation bar includes tabs for Dashboard, ACC, Monitor, Policies (which is selected), Objects, Network, Device, Commit, Config, and Search.

Team B:  
Grant Arnold  
Mehmett Ozman  
Jackson Pence  
Andre Davis

## NAT Hits:

The screenshot shows the Palo Alto Networks Management Console interface. The top navigation bar includes File, Action, Media, Clipboard, View, Help, and tabs for Dashboard, ACC, Monitor, Policies (selected), Objects, Network, Device, Commit, Config, and Search. The left sidebar has sections for Security, NAT (selected), QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection, and SD-WAN. The main content area displays a table titled "Rule Usage" under the "Policy Optimizer" section. The table has columns: Destination Translation, Hit Count, Last Hit, First Hit, Modified, and Created. There are four rows in the table, all showing "none" in the Destination Translation column and "0" in the Hit Count column. The Last Hit, First Hit, Modified, and Created columns show dates and times from February 2, 2022, at 03:32:39. The bottom of the screen shows a toolbar with various icons and a status bar indicating "Status: Running".

Rule Usage						
Destination Translation	Hit Count	Last Hit	First Hit	Modified	Created	
none	8	2022-02-02 03:35:30	2022-02-02 03:32:39	2022-02-02 03:32:23	2022-02-02 03:32:23	
none	7	2022-02-02 03:35:30	2022-02-02 03:32:39	2022-02-02 03:32:23	2022-02-02 03:32:23	
none	0	-	-	2022-02-02 03:32:23	2022-02-02 03:32:23	
none	0	-	-	2022-02-02 03:32:23	2022-02-02 03:32:23	

Team B:  
Grant Arnold  
Mehmett Ozman  
Jackson Pence  
Andre Davis

## Security Policies For Second Firewall:

The screenshot shows the Palo Alto Networks UI interface. The top navigation bar includes File, Action, Media, Clipboard, View, Help, and tabs for Dashboard, ACC, Monitor, Policies (selected), Objects, Network, Device, Commit, Config, and Search. The main content area displays a table of security policies under the 'Security' category. The table has columns for Name, Tags, Type, Zone, Address, User, HIP Profile, and Zone. There are five items listed:

	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone
1	Internet NAT	none	universal	inside	any	any	any	outside
2	DMZ-NAT	none	universal	dmz	any	any	any	outside
3	egress-outside	none	universal	inside	any	any	any	outside
4	intrazone-default	none	intrazone	any	any	any	any	(intrazone)
5	interzone-default	none	interzone	any	any	any	any	any

The left sidebar shows other policy categories like NAT, QoS, Policy Based Forwarding, Decryption, Tunnel Inspection, Application Override, Authentication, DoS Protection, and SD-WAN. A 'Policy Optimizer' section lists unused apps and rule usages. The bottom navigation bar includes tabs for Addresses, Buttons, Overrides, Revert, Enable, Disable, Move, PDF/CSV, Highlight Unused Rules, Reset Rule Hit Counter, Group, Tasks, Language, and a status bar showing admin, Logout, Last Login Time: 02/02/2022 03:11:07, and system time: 10:34 PM, 2/1/2022.

Team B:  
Grant Arnold  
Mehmett Ozman  
Jackson Pence  
Andre Davis

## Security Policy (Hit Count):

The screenshot shows the Palo Alto Networks Management Console interface. The main window displays the 'Rule Usage' table under the 'Policies' tab. The table has columns for Options, Hit Count, Last Hit, First Hit, Apps Seen, Days with No New Apps, and Modified. There are five items listed:

Options	Hit Count	Last Hit	First Hit	Apps Seen	Days with No New Apps	Modified
	10	2022-02-02 03:34:24	2022-02-02 03:34:24	-	-	2022-02-02 03:32:23
	9	2022-02-02 03:34:24	2022-02-02 03:34:24	-	-	2022-02-02 03:32:23
	0	-	-	-	-	2022-02-02 03:32:23
none	28324	2022-02-02 03:32:10	2022-01-28 20:14:45	-	-	2022-01-13 13:47:43
none	109440	2022-02-02 03:32:12	2022-01-28 20:14:45	-	-	2022-01-13 13:47:43

The left sidebar shows the 'Security' category with various policy-based forwarding options like NAT, QoS, and Policy Based Forwarding. The 'Policy Optimizer' section shows counts for 'No App Specified' (0), 'Unused Apps' (0), and 'Rule Usage' (3). The bottom navigation bar includes links for Logout, PDF/CSV, and Reset Rule Hit Counter.

Team B:  
Grant Arnold  
Mehmett Ozman  
Jackson Pence  
Andre Davis

## PfSense Screenshots:

### PfSense Configuration Pt.1

Here we added a packet capture rule in order to capture any traffic coming into and out of the server.

The screenshot shows a web browser window titled "4777B01Honey on SecNet - Virtual Machine Connection". The URL in the address bar is "https://192.168.72.22/diag\_packet\_capture.php". The page displays the "Diagnostics / Packet Capture" configuration screen. The "Packet Capture Options" section includes fields for "Interface" (set to "WAN"), "Promiscuous" mode (unchecked), "Address Family" (set to "Any"), "Protocol" (set to "Any"), and "Host Address" (empty). A detailed description of the host address field is provided, explaining CIDR notation, subnet掩码, and MAC address formats. The browser's status bar at the bottom indicates "Status: Running".

Team B:  
Grant Arnold  
Mehmett Ozman  
Jackson Pence  
Andre Davis

## PfSense Configuration Pt.2 (Packet Capture Rule Creation)

The screenshot shows the 'diag\_packet\_capture.php' configuration page on a pfSense web interface. The page title is 'pfSense.home.apa - Diagnostic'. The URL in the address bar is 'https://192.168.72.22/diag\_packet\_capture.php'. The main content area contains several configuration fields:

- Port:** A text input field with a placeholder for specifying a port number.
- Packet Length:** A text input field set to '0', indicating no length filtering.
- Count:** A text input field set to '100', indicating the number of packets to capture.
- Level of detail:** A dropdown menu set to 'Normal'.
- Reverse DNS Lookup:** A checkbox labeled 'Do reverse DNS lookup' which is unchecked. A note below states: 'The packet capture will perform a reverse DNS lookup associated with all IP addresses. This option can cause delays for large packet captures.'
- Last capture start:** A timestamp showing 'February 2nd, 2022 2:35:00 am.'
- Last capture stop:** A timestamp showing 'February 2nd, 2022 2:37:57 am.'

At the bottom, there are three buttons: 'Start' (green), 'View Capture' (blue), and 'Download Capture' (blue). Below the buttons is a progress bar titled 'Packets Captured'.

The system tray at the bottom shows the status as 'Running' and includes icons for the Start button, search, file explorer, browser, settings, and system status. The system status bar shows the time as '9:40 PM' and date as '2/1/2022'.

Team B:  
Grant Arnold  
Mehmett Ozman  
Jackson Pence  
Andre Davis

### Packets Being Captured: Successful Packet Pull and Internet is up and running

```
PACKETS CAPTURED
```

```
02:36:19.674663 IP 192.168.72.22 > 192.168.72.254: ICMP echo request, id 44366, seq 1441, length 9
02:36:19.676418 IP 192.168.72.254 > 192.168.72.22: ICMP echo reply, id 44366, seq 1441, length 9
02:36:20.216145 IP 192.168.72.22 > 192.168.72.254: ICMP echo request, id 44366, seq 1442, length 9
02:36:20.217985 IP 192.168.72.254 > 192.168.72.22: ICMP echo reply, id 44366, seq 1442, length 9
02:36:20.757547 IP 192.168.72.22 > 192.168.72.254: ICMP echo request, id 44366, seq 1443, length 9
02:36:20.758495 IP 192.168.72.254 > 192.168.72.22: ICMP echo reply, id 44366, seq 1443, length 9
02:36:21.298773 IP 192.168.72.22 > 192.168.72.254: ICMP echo request, id 44366, seq 1444, length 9
02:36:21.300190 IP 192.168.72.254 > 192.168.72.22: ICMP echo reply, id 44366, seq 1444, length 9
02:36:21.834928 IP 192.168.72.22 > 192.168.72.254: ICMP echo request, id 44366, seq 1445, length 9
02:36:21.836415 IP 192.168.72.254 > 192.168.72.22: ICMP echo reply, id 44366, seq 1445, length 9
02:36:22.344690 IP 192.168.72.22 > 192.168.72.254: ICMP echo request, id 44366, seq 1446, length 9
02:36:22.346160 IP 192.168.72.254 > 192.168.72.22: ICMP echo reply, id 44366, seq 1446, length 9
02:36:22.886196 IP 192.168.72.22 > 192.168.72.254: ICMP echo request, id 44366, seq 1447, length 9
02:36:22.886907 IP 192.168.72.254 > 192.168.72.22: ICMP echo reply, id 44366, seq 1447, length 9
02:36:23.427541 IP 192.168.72.22 > 192.168.72.254: ICMP echo request, id 44366, seq 1448, length 9
02:36:23.428794 IP 192.168.72.254 > 192.168.72.22: ICMP echo reply, id 44366, seq 1448, length 9
02:36:23.968991 IP 192.168.72.22 > 192.168.72.254: ICMP echo request, id 44366, seq 1449, length 9
02:36:23.970355 IP 192.168.72.254 > 192.168.72.22: ICMP echo reply, id 44366, seq 1449, length 9
02:36:24.023153 IP 192.168.72.22.2477 > 192.168.74.113.443: tcp 1
02:36:24.024247 IP 192.168.74.113.443 > 192.168.72.22.2477: tcp 0
02:36:24.024367 IP 192.168.74.113.443 > 192.168.72.22.2477: tcp 0
```