|  |  |
| --- | --- |
| **Network Security**  Diploma in CSF  Year 3 (2020/21) Semester 5 | Week 4 |
| Tutorial |
| **Application Identification** | |

1. Research and explain how Ingress and Egress filtering are able to mitigate spoofing.

|  |
| --- |
| Ingress filtering - When an internal LAN address appears as a source address in a packet on its way into a network from outside - this is a spoofed address  Egress filtering - If a packet with a source address from the outside such as an Internet address is received by a firewall from an interface inside the private LAN -then this is a spoofed address. |

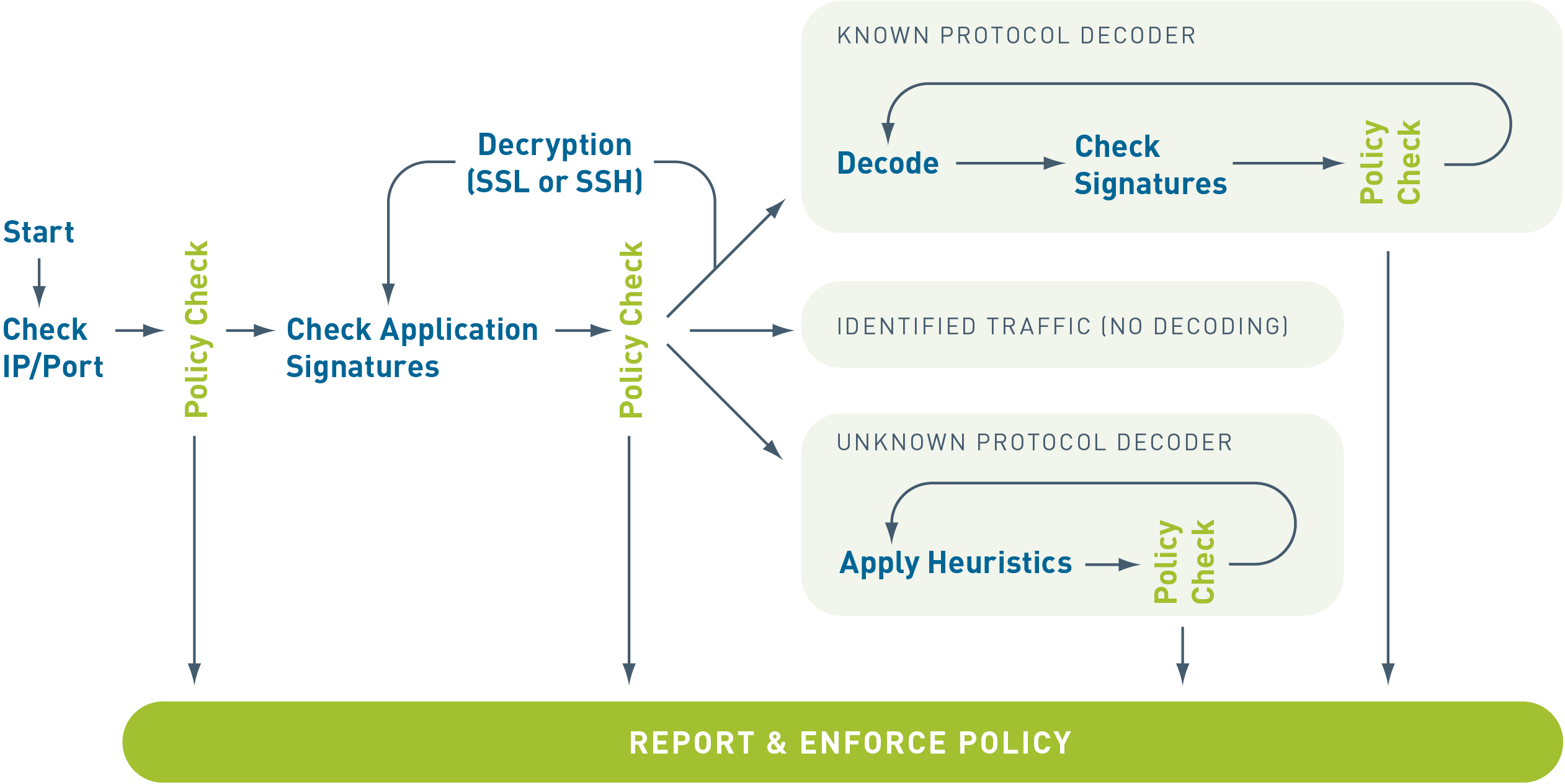
1. Compare the 3 types of Source NAT: Port Address Translation, Static NAT, and Dynamic NAT.

|  |
| --- |
| Refer to Week 3 Lecture, slide 17.   * Dynamic IP/Port (Port Address Translation)   + Multiple clients use the same public IP addresses with different source port numbers   + Assigned address can be set to Interface address or Translated address * Dynamic IP   + 1-to-1 translations   + Private source addresses translate to the next available address in the range   + Source port is unchanged * Static IP   + 1-to-1 fixed translations   + Use static IP to change the source IP address while leaving the source port unchanged |

1. Describe Destination NAT (Reverse Proxy or Reverse NAT).

|  |
| --- |
| Refer to week 3 lecture, slide 18.  Destination address translation is used to map a single public IP address to multiple private servers and services, destination ports can stay the same or be directed to different destination ports. |

1. Based on the Application Filtering Flow diagram, describe how App-ID identifies applications crossing your network.



|  |
| --- |
| • Traffic is first classified based on the IP address and port.  • Signatures are then applied to allowed traffic to identify the application based on unique application properties and related transaction characteristics.  • If App-ID determines that encryption (SSL or SSH) is in use, and a decryption policy is in place, the application is decrypted and application signatures are applied again on the decrypted flow.  • Decoders for known protocols are then used to apply additional context-based signatures to detect other applications that may be tunneling inside of the protocol (e.g., Yahoo! Instant Messenger used across HTTP).  • For applications that are particularly evasive and cannot be identified through advanced signature and protocol analysis, heuristics or behavior analysis may be used to determine the identity of the application.  As the applications are identified by App-ID's successive mechanisms, the policy check determines how to treat the applications and associated functions: block them, allow them and scan for threats, inspect for unauthorized file transfer and data patterns, or shape using QoS. |

1. What do you understand by the term security policy dependencies? Draw a diagram to illustrate.

|  |
| --- |
| Many applications rely on other applications to be running before they can be used. In a Palo Alto Networks firewall environment, you must make sure that an application's parent applications are allowed in order for your target application to function correctly.  For example, a user wants Use Google Translate. Applications accessed through a web browser will first be recognized as an HTTP session. The administrator will have to enable the web-browsing application in addition to allowing the google-translate-base application.  Application dependencies can be found by accessing App-ID in the GUI. Click Objects > Applications to see application information. The App-ID listings are also available through Applipedia. |