**Defense in depth** is a philosophy that provides layered security to a system by using multiple security mechanisms and generally follows these principles:

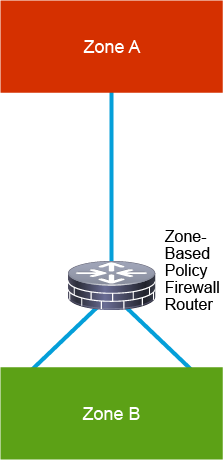
* Security mechanisms should back each other up and provide diversity and redundancy of protection.
* Security mechanisms should not depend on each other, so that their security does not depend on other factors that are outside their control.
* Using defense in depth, you can eliminate single points of failure and augment weak links in the system to provide stronger protection with multiple layers

**Stateful Firewall**

* A firewall is a network security device that monitors the incoming and outgoing network traffic and decides whether to allow or block the traffic based on a defined set of security rules.
* Firewalls establish a barrier between the secured and controlled internal networks that can be trusted, and the untrusted outside networks, such as the Internet.
* Stateful firewall: Cisco Adaptive Security Appliance (ASA) or Cisco Firepower NGFW
* Stateful firewalls inspect all activity from the opening of a connection until the connection is closed.
* Data that is associated with each connection is stored in the firewall connection's state table.
* A state table, which is an internal data structure of a stateful packet filter, tracks all OSI Layer 4 sessions and inspects all packets that are passing through the device
* Advanced stateful firewalls, such as the Cisco ASA, also offer features such as network address translations (NAT), identity-based access controls, applications layer inspections, VPN capabilities, and botnet traffic filtering.

**Cisco IOS Zone-Based Policy Firewall Overview**

* The Zone-Based Policy Firewall is a Cisco IOS Software feature that allows a router to act as a powerful and flexible stateful firewall between zones that correspond to security domains that are created through network separation.
* A Zone-Based Policy Firewall zone is a collection of networks that are reachable over one or more specific router interfaces that are designated to belong to the same zone.
* Zone-Based Policy Firewall access control policies then control access between two or more zones that are configured on the router, using a flexible configuration language that allows you to specify simple or complex access policies in a manageable manner.
* Router interfaces are assigned to security zones, and firewall inspection policy is applied to traffic moving between the zones.
* Zone-Based Policy Firewall enforces a secure inter-zone policy by default, such that a given interface cannot pass traffic to interfaces in other security zones until an explicit policy allowing traffic is defined.



**Security Intelligence Overview** (renseignement de sécurité, le renseignement sur les menaces)

* Security Intelligence, threat intelligence, cyber threat intelligence, or "intel" for short is an important tool in preventing cyber-attacks. Gartner has defined threat intelligence as: "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject’s response to that menace or hazard."
* Many security intelligence services provide automatic updates that include dynamic lists of known Command and Control (CnC) servers, dangerous Uniform Resource Identifiers (URIs), or lists of known malicious hosts.
* The use of security intelligence is a typical feature available in today's next-generation firewalls, and it works by blocking traffic to or from IP addresses that have a known bad reputation.
* This traffic filtering takes place before any other policy-based inspection, analysis, or traffic handling.
* Cisco Talos Intelligence Group is one of the threat intelligence leaders in the market. Talos Intelligence Group is composed of leading threat researchers that create threat intelligence for Cisco products to protect customers from both known and emerging threats.

**Threat Information Standardization**

* Over the past years, cyber-attacks have become increasingly common and sophisticated.
* Sharing of threat information between organizations becomes a key priority
* Threat information needs to be standardized and structured
* **STIX (Structured Threat Information Expression)** is used to share threat data, so called Cyber Threat Intelligence (CTI).
* **TAXII** is a transport mechanism for sharing cyber threat intelligence and is the preferred exchange mechanism for STIX (protocol).
* TID is a feature on Cisco’s Firepower Management Center (FMC) product offering that automates the operationalization of threat intelligence. TID has the ability to consume threat intelligence via STIX over TAXII and allows uploads and downloads of STIX and simple blocked lists.

**Network-Based Malware Protection Overview**

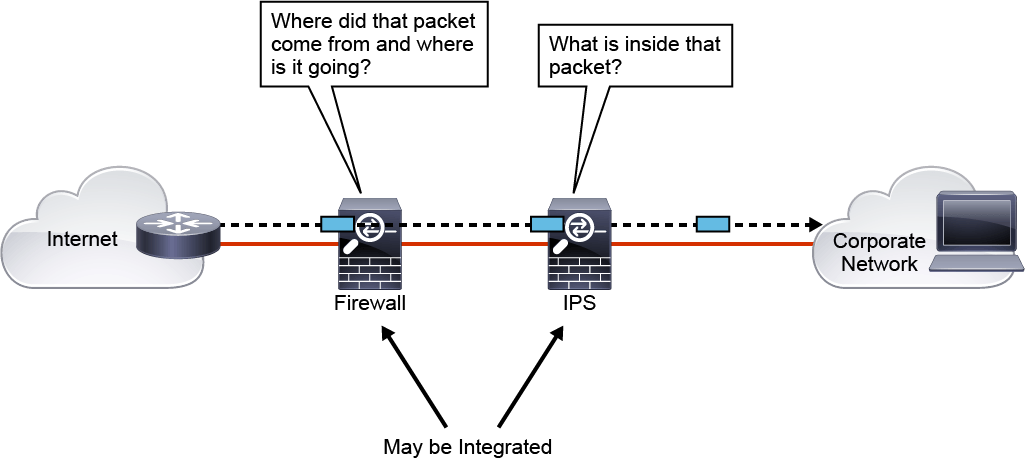
* Network-based malware protection prevents malware files from being transmitted through the network security device such as a Firepower next-generation firewall, Cisco Email Security Appliance (ESA), Cisco Web Security Appliance (WSA), and Cisco Umbrella
* Whether files arrive from the web, email, or other attack vectors, the system automatically recognizes files and applications

**IPS Overview**

* Intrusion sensors are systems that detect activity that can compromise the confidentiality, integrity, and availability of information resources, processing, or systems.
* An IPS has the ability to analyze traffic from the data link layer to the application layer.

For example, an IPS can:

* Analyze the traffic that controls Layer 2 to Layer 3 mappings, such as Address Resolution Protocol (ARP) and DHCP.
* Verify that the rules of networking protocols such as IP, TCP, UDP, and Internet Control Message Protocol (ICMP) are followed.
* Analyze the payload of application traffic to identify things such as network attacks, the presence of malware, and server misconfigurations.
* IPS can identify, stop, and block attacks that would normally pass through a traditional firewall device.
* The essential **difference between an IDS and an IPS** is that an IPS can respond immediately, and prevent possible malicious traffic from passing.
* An IDS simply produces alerts when suspicious traffic is seen. An IDS is not responsible for mitigating the threat.



* firewall controls access based on source and destination IP addresses and ports, while the IPS controls access based on packet payload. An IPS also has other valuable capabilities, such as providing deeper insight into what is actually happening on your network.

IPS technology is deployed in a sensor, which is variously described as one of the following:

* An appliance that is specifically designed to provide dedicated IPS services. Cisco provides Cisco Firepower device, which offers many different capabilites, IPS being just one of them.
* A module that is installed in another network device, such as an adaptive security appliance, a switch, or a router. Cisco provides Firepower services module that can be installed in Cisco ASA.

Intrusion detection technology uses different strategies to detect and mitigate against attacks:

* **Anomaly detection:** This type of technology generally learns patterns of normal network activity and, over time, produces a baseline profile for a given network. Sensors detect suspicious activity by evaluating patterns of activity that deviate from this baseline.
* **Rule-based detection**: Malicious activity detectors typically analyze live network traffic using a database of IPS rules (or also called IPS signatures) to determine whether suspicious activity is occurring.
* **Reputation-based:** Reputation-based filtering allows the IPS to block all traffic from known bad sources before any significant inspection is done.

**Next Generation Firewall Overview**

NGFW performs various security functions trying to protect the network from advanced attacks

Let's look at some of the typical next generation requirements of a next-generation firewall.

* **Granular application visibility and control:** Example, allowing instant messaging (IM) but blocking file transfers over IM
* **Intrusion prevention system**: Example, identify and potentially block malicious data that is carried in network sessions.
* **Reputation**-**based filtering:** Example, automatic blocking to suspected bad web sites
* **Enforce acceptable user policy:** Example, blocking employees from browsing to unacceptable web sites
* **SSL/TLS traffic decryption:** Example, decrypting Facebook traffic so it can be inspected and controlled
* **User- or user group**-**based policies:** Example, allowing only the engineering employees to access the development servers
* **Real-time contextual awareness:** Example, automatic passive network, hosts, operating systems, applications, and users discoveries
* **Intelligent security automation:** Example, automatic correlation of different events data and impact assessment

Email Content security okkk