



Romel Cabiling ▾



[Home](#)

[Home](#) > [My courses](#) > [121 - ITSP2B](#) > [03 Intrusion Prevention System](#) > [Lesson Proper for Week 3](#)

Lesson Proper for Week 3

Prevention

The IPS often sits directly behind the firewall and provides a complementary layer of analysis that negatively selects for dangerous content. Unlike its predecessor the Intrusion Detection System (IDS)—which is a passive system that scans traffic and reports back on threats—the IPS is placed inline (in the direct communication path between source and destination), actively analyzing and taking automated actions on all traffic flows that enter the network.

Specifically, these actions include:

- Sending an alarm to the administrator (as would be seen in an IDS)
- Dropping the malicious packets
- Blocking traffic from the source address
- Resetting the connection

As an inline security component, the IPS must work efficiently to avoid degrading network performance. It must also work fast because exploits can happen in near real-time. The IPS must also detect and respond accurately, so as to eliminate threats and false positives (legitimate packets misread as threats).

Detection

The IPS has a number of detection methods for finding exploits, but signature-based detection and statistical anomaly-based detection are the two dominant mechanisms.



Signature-based detection is based on a dictionary of uniquely identifiable patterns (or signatures) in the code of each exploit. As an exploit is discovered, its signature is recorded and stored in a continuously growing dictionary of signatures. Signature detection for IPS breaks down into two types:

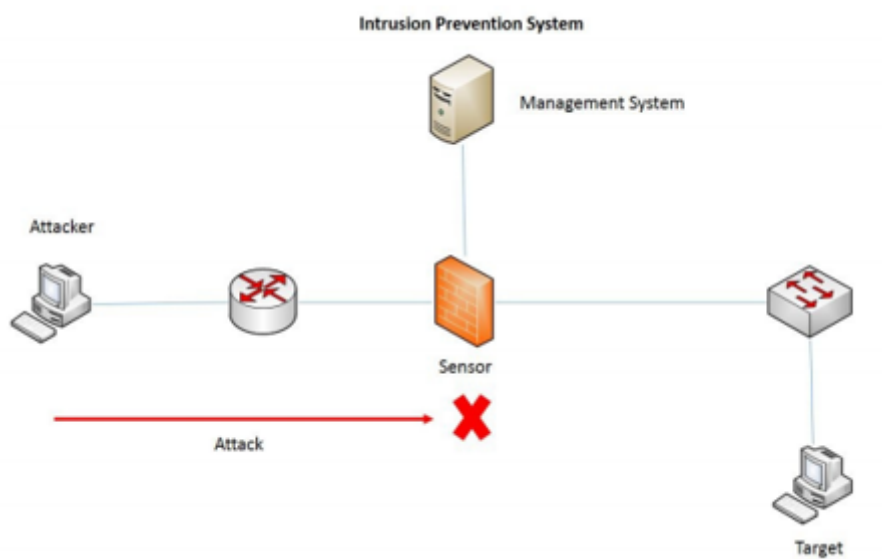
1. Exploit-facing signatures identify individual exploits by triggering on the unique patterns of a particular exploit attempt. The IPS can identify specific exploits by finding a match with an exploit-facing signature in the traffic stream
2. Vulnerability-facing signatures are broader signatures that target the underlying vulnerability in the system that is being targeted. These signatures allow networks to be protected from variants of an exploit that may not have been directly observed in the wild, but also raise the risk of false positives.

Statistical anomaly detection takes samples of network traffic at random and compares them to a pre-calculated baseline performance level. When the sample of network traffic activity is outside the parameters of baseline performance, the IPS takes action to handle the situation.

IPS was originally built and released as a standalone device in the mid-2000s. This however, was in the advent of today's implementations, which are now commonly integrated into Unified Threat Management (UTM) solutions (for small and medium size companies) and next-generation firewalls (at the enterprise level).

INTRUSION PREVENTION SYSTEM

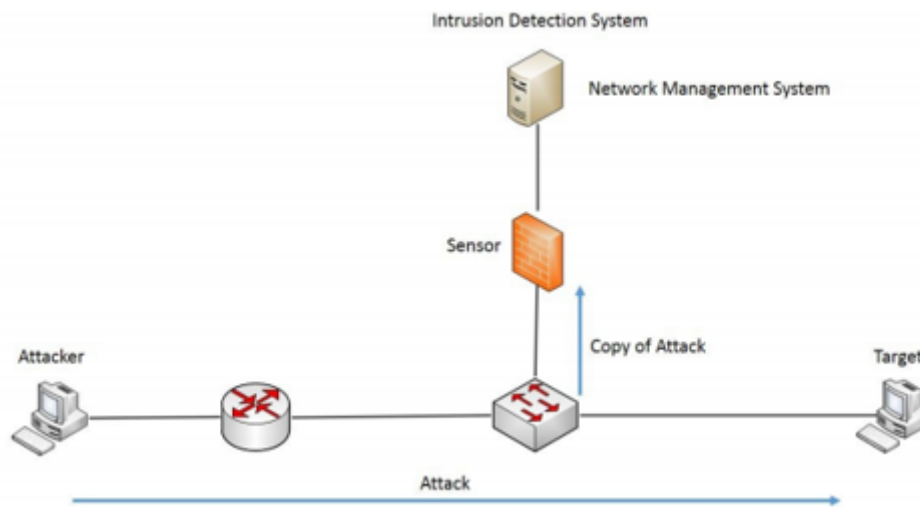
An intrusion prevention system (IPS) is a proactive methodology to understand potential threats, stop attacks inline, and report them immediately. An IPS is a module or an individual device that can look into the payload of the traffic coming from the outside zone, thereby ensuring that any malicious traffic would be blocked inline:



INTRUSION DETECTION SYSTEM

An intrusion detection system (IDS) is a monitoring system that passively monitors incoming and outgoing network traffic for suspicious attacker activity. An IDS is a module that can alert network devices, but it cannot stop attacks from happening. Generally, an IDS is configured in promiscuous mode because it cannot block the attacks, but it can send alerts:





One major question you may have is how different is an IPS from a firewall that can also do deep-packet inspection? Well, the answer is that an IPS can identify traffic patterns that might match an attack, while a firewall can do an inspection on a per-packet basis, thereby they would not be intelligent enough to detect an attack. So, in any secure network, an IPS complements a firewall.

The different IPS and IDS identification methods are discussed here:

- **Signature-based:** The IPS verifies the traffic pattern against a database of well-known attacks referred to as signatures. If a particular traffic pattern matches the signature, it will trigger the signature.
- **Policy-based:** In this method, the IPS identifies any traffic outside the defined policy as malicious and blocks it.
- **Anomaly-based:** This method depends on a traffic baseline that is created based on observations made over a certain period of time.
- **Reputation-based:** This is a method that correlates all the different attacks across the globe and tries to verify the traffic pattern using that correlated database.
- **HIPS:** A host-based IPS is used on an individual machine instead of the entire network. This might be equivalent to an antivirus, but can analyze the attacks with a higher capability than an antivirus. This is of course operating system-dependent.

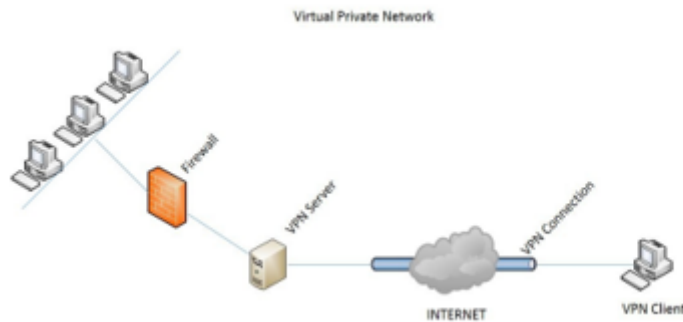
VIRTUAL PRIVATE NETWORK

A Virtual Private Network (VPN) is an extension of a private network into the public network domain. The public network would act as a private network and the user would be able to perform every function as if logged in to the private network. It also helps to allow a remote user to work with the same security and management policies defined by the administrator of the private network. This connection is established by a virtual point-to-point connection through a set of assigned connections and encryption, or a combination of both, depending on the business requirements.



VPNs allow employees to securely log in to their private network, even if they are not in their office premises. It is secure and cost-effective.

Any kind of network connection over an untrusted network, such as the internet, would benefit from implementing a VPN. Even inside an organization's premises, in order to implement a VPN, you need to create a secure private channel between network devices (site-to-site VPN), as well as between people and network devices (remote-access VPN):



1. Benefits of VPN

A VPN can benefit the organization in the following ways:

- **Eliminating the need for long-distance leased lines:** Organizations need to rent network capacity, such as T1/E1 lines, to achieve full, secured network connectivity between their office locations. A VPN would allow the user to log in to the private network using the public network, so there is no requirement for the company to procure a leased line. These connections can be tapped into the virtual network through much cheaper internet connectivity options, such as broadband connections.
- **Reducing long-distance call charges:** A VPN would also enable the user to use VoIP services in a secured manner, thereby skipping logging in to the remote-access server by the business travelers who need to access the company's intranet. For example, with an internet VPN, clients need to connect to the nearest service provider's access point.

2. Site-to-site VPN

A site-to-site VPN allows offices in multiple fixed location to establish a secure connection with each other over a public network, as shown in the following topology, with a lot of security measures bundled in. This enables the company's resources and data to be available to branch offices in other locations. For example, the server in the headquarters can be accessed securely by branch users:



The two sites, using their VPN edge devices, set up the IPSEC VPN tunnel, which includes security parameters such as encryption algorithm, hashing algorithm, and authentication. Once the tunnel is established, the data from the LAN of the head office would be sent through the secured tunnel to the LAN of the branch office.

There are two types of site-to-site VPN:

- Internet-based: When a company has several branches located in different areas and they wish to join all of them as one private network, then they can connect each LAN to a single WAN.
- Extranet-based: When a company has to work very closely with their partners, vendors, or customers, then they can have an extranet VPN to build a connection that would require LAN connectivity. In this scenario, they can work in a secured manner by ensuring that all the data required is accessible and it also prevents access to their internal network.

3. Remote-access VPN

A Remote-access VPN is also called a **VPDN**, or **virtual private dial-up network**.

Similar to the site-to-site access evolution from WAN technologies, remote access has evolved from dial-up technology. The differentiating factors between these two types of VPN are:

- Remote-access VPN clients initiate the VPN on-demand
- The remote-access client requires the Cisco VPN client software to connect
- Remote-access uses a server client mechanism where the server authenticates first

This can be very flexible when implemented as a software solution on a remote user's PC. The teleworker can benefit from the same confidentiality, integrity, and authentication services of a site-to-site VPN.

It allows individual users to establish a secure connection with a remote computer network. They can access only the secured resources or data on that particular network, as if they were directly connected with the network. For example, a company where there are hundreds of sales personnel out in the field trying to access information from their sales servers can use a remote-access VPN:



There are two components in a remote-access VPN:



Network access server (NAS): Also known as media gateway or remote access server. NAS is a dedicated server that has multiple applications running in it. Users initially connect to the NAS server in order to get connected to the VPN. NAS also provides its own authentication services.

VPN client software: This helps users to access their data via VPN. The client software establishes and maintains the connection with the NAS server. The modern operating system comes with a few built-in VPN applications; others must install third-party software specific to their organization's VPN configurations. The NAS, using a third-party Certificate Authority (CA), gets its digital certificate, which it will use to prove its identity to the client. Once successfully authenticated, the client software creates a tunnel connection to the NAS server, which is indicated by the user's IP address. The client software maintains the security level by using encryption standards, such as Secure Socket Layer (SSL).

◀ Preliminary Activity for Week 3

Jump to...



Analysis, Application, and Exploration for Week 3 ▶



Navigation

Home

 Dashboard

Site pages

My courses

121 - CC106

121 - BPM101 / DM103

121 - OAELEC2

121 - ITE3

121 - MUL101

121 - ITSP2B

Participants



Grades

General


01 Exploring Security Threats

02 Delving into Security Toolkits

03 Intrusion Prevention System

 Preliminary Activity for Week 3

 **Lesson Proper for Week 3**

 Analysis, Application, and Exploration for Week 3

 Generalization for Week 3

 Evaluation for Week 3

 Assignment for Week 3

04 Understanding Security Policies I



05 Understanding Security Policies II
06 - Preliminary Examination
07 Deep Diving into Cryptography
08 Deep Diving into Cryptography: Types of Cipher
09 Implementing the AAA Framework
10 Implementing the AAA Framework: Implementing A...
11 Securing the Control and Management Planes
12 - Midterm Examination
13 Protecting Layer 2 Protocols
14 Protecting the Switch Infrastructure
15 Exploring Firewall Technologies I
16 Exploring Firewall Technologies II
17 Cisco ASA
121 - WEB101 / CCS3218
Courses

Fair Warning

NOTICE: Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.***

PROSECUTION: Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

COURSE OF ACTION: Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

2nd Semester Enrollment



A banner for Bestlink College of the Philippines (BCP) featuring a blue-tinted image of a modern building. The text is overlaid in white and red. At the top right, it says "visit www.bcp.edu.ph". The main headline in large red letters reads "Enrollment registration is now Ongoing". Below this, in white text on a blue background, it says "For 2nd Semester SY 2021 - 2022". Underneath, in white text on a dark blue background, it says "We are accepting new students, returnees and transferees." On the right side, there is a quote: "Be trained to be the best, Be linked to success" next to a circular logo. At the bottom left, there is an email icon and the address "bcp-inquire@bcp.edu.ph". At the bottom right, there is a phone icon and the numbers "(8)442-8601 | (8)518-8050".

visit www.bcp.edu.ph

Enrollment registration is now Ongoing

For 2nd Semester SY 2021 - 2022





We are accepting new students, returnees and transferees.

"Be trained to be the best,
Be linked to success"

 bcp-inquire@bcp.edu.ph

 (8)442-8601 | (8)518-8050

Activities

-  Assignments
-  Forums
-  Quizzes
-  Resources

Bestlink College of the Philippines
College Department

Powered by [eLearning Commons](#)

