Deploying IPS Using the Cisco ASA AIP-SSM

IPS TME Architecture Team

January 25, 2008

Introduction

This design guide explains the requirements of deploying a Cisco ASA Advanced Inspection and Prevention Security Services Module (AIP-SSM) inside the Cisco ASA security appliance. The software version used in this discussion will be Cisco ASA Software Version 8.0.x code for the appliance, and Cisco IPS Sensor Software 6.1.x code for the AIP-SSM.

This document is broken up into three parts.

- AIP-SSM deployment overview
- Normalizer revisited and comparison of signature and session states
- Typical Cisco ASA appliance installations and deployment concerns for the AIP-SSM

Part 1 AIP-SSM Deployment Overview

The Cisco ASA 5500 Series AIP-SSM is an inline, network-based solution that accurately identifies, classifies, and stops malicious traffic before it affects business continuity. It combines inline prevention services with innovative technologies, resulting in total confidence in the provided protection of the deployed IPS solution, without the fear of legitimate traffic being dropped. The AIP-SSM also offers comprehensive network protection through its unique ability to collaborate with other network security resources, providing a proactive approach to protecting the network. It uses accurate inline prevention technologies that provide unparalleled confidence to take preventive action on a broader range of threats without the risk of dropping legitimate traffic. These unique technologies offer intelligent, automated, contextual analysis of data and help ensure that businesses are getting the most out of their intrusion prevention systems (IPSs). Furthermore, the AIP-SSM uses multivector threat identification to protect the network from policy violations, vulnerability exploitations, and anomalous activity through detailed inspection of traffic in Layers 2 through 7.

Deploying the AIP-SSM into an existing deployment is straightforward in most regards. Since the AIP-SSM doesn't actually function as a separate device in the network, there are no changes required to network topology. All that is required is to physically insert the module, initialize it, and then create a policy in the appliance's configuration to define which traffic and what specific type of traffic gets sent to the module for analysis and then how that traffic gets analyzed (IDS vs. IPS mode).

Part 2 Comparing Signature and Session States, and Revisiting the Normalizer

Failover events are important events for network devices that track and enforce state because sessions that are not known by a device might get dropped. There are two types of state that need to be discussed in this context: session state and signature state.

- Session state consists of pieces of information required to track TCP/IP sessions and ensure that they conform to the correct standards and that packets seen on the wire actually belong to one session or another. Pieces of data routinely but not always tracked by every device include source (src) and destination (dst) IP addresses and ports (TCP and UDP but not ICMP; the combo of src and dst IP is known as a dual src/dst IP and src/dst port is known as a quad). For TCP connections, additional data might be sequence number, TCP window size, PAWS information, TTL, and others. Using this information, a stateful device in the middle can accurately enforce TCP/IP state on traversing packets. Without this information, it is difficult to tell when evasion techniques are being used to try and hide malicious activity. The Cisco ASA appliance shares session state in a high-availability deployment. The IPS standalone devices and modules currently do not.
- Signature state is the information currently stored for various detection algorithms. It is built up from seeing a complete connection as it traverses the device. Signature state, unlike session state, can actually be larger than the packet that generated it. This can be because a single packet can generate state for many different algorithms. For example, a single SYN packet on port 80 can initiate state for algorithms looking for atomic attacks, sweeps and floods, TCP attacks, and HTTP attacks. For this reason, IPS devices either don't share signature state or they share the whole packet stream between devices.

The TCP/IP normalizer is a portion of code built to analyze packets and build session and signature state on the data it sees in each packet. It tracks this data to ensure that subsequent packets are valid and actually part of the flows that they might seem to be on first inspection. The normalizer also performs these actions to prevent the sensor from being fooled or blinded to malicious activity by someone using various techniques. The basis for discussing some of these obfuscation techniques was discussed in a paper available here Insertion, Evasion, and Denial of Service: Eluding Network Intrusion Detection (1998).

These same techniques then were incorporated into numerous tools, starting with Fragrouter (and followed with fragroute) and others.

One of the many functions of the normalizer is to identify and potentially stop malicious users from using these techniques to try and evade detection. One of the more common activities of the normalizer is to identify and potentially drop when a packet is seen that is not a SYN packet and not part of any existing connection being tracked. Another function is to identify and potentially stop a packet that is supposed to be part of an existing connection (the dual matches) but doesn't match other key criteria (sequence number doesn't match, outside the TCP window size, etc.). These functions occur in the appliance by default and are an important part of the standalone devices activities.

In the Cisco ASA appliance, the AIP-SSM does not run the normalizer code and does not track and enforce session state. Instead, the module depends entirely on the appliance for providing that same level of function and protection. Because of this, there is less of a requirement for the AIP-SSMs to share state between themselves for failover situations, as it will not block existing sessions as they move over to the new appliance (since the appliance itself will know about the new session).

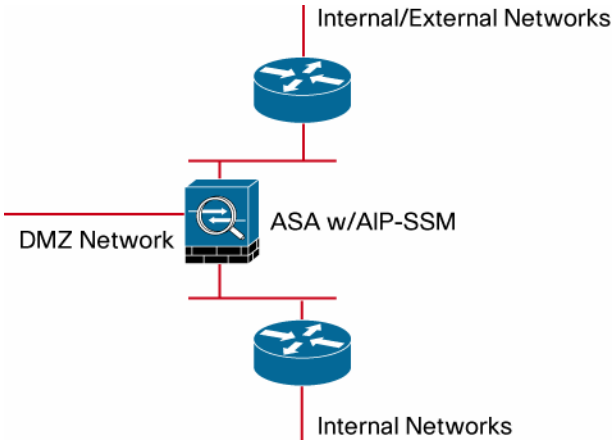
Part 3 Deployment Scenarios

This section covers three specific deployment scenarios and how an AIP-SSM should be deployed and configured in these examples, along with possible caveats.

Single Appliance

The first deployment is the single Cisco ASA appliance in a non-high-availability deployment (Figure 1). This is the most straightforward Cisco ASA deployment, where a single appliance is used to segment different networks. In this example, the Cisco ASA appliance sits between the Internet and the DMZ and internal networks.

Figure 1. Single Adaptive Security Appliance

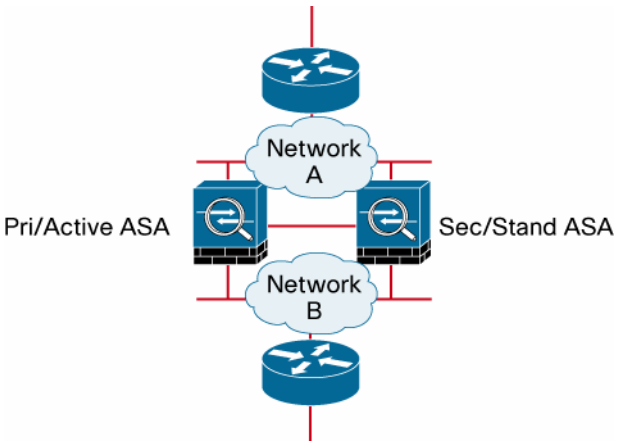


Putting a Cisco ASA appliance into this deployment is simple: the only concern is defining the traffic policy. Example policies might be to inspect traffic from outside to the DMZ, or inside in IPS mode and traffic from inside to DMZ or outside in IDS mode.

Pair of Appliances

The second deployment option a pair of Cisco ASA appliances in an active-passive high-availability deployment (Figure 2).

Figure 2. Appliances in Active-Passive Deployment



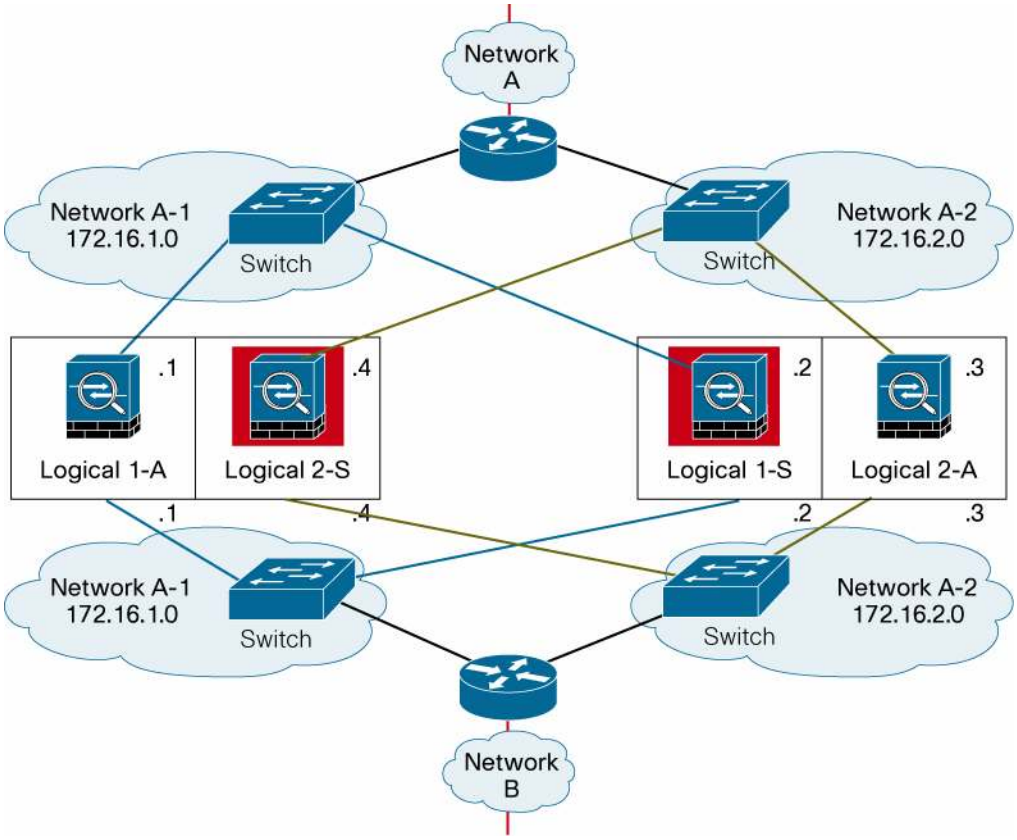
Putting AIP-SSMs into this deployment is quite simple as well. In this design, traffic always flows in and out of a single Cisco ASA appliance, whichever is active at the time. Since the appliance is responsible for tracking and enforcing session state, the normalizer in the AIP-SSM isn't included

in the processing path and is basically disabled. This means that from the AIP-SSM's perspective, anything that gets passed to it for analysis has been cleared by the appliance as being valid and correct. As long as the high-availability solution is functioning correctly, all session state will be shared to the passive Cisco ASA appliance so when a failover event occurs, the backup appliance takes over session management and packets start flowing through it without issue. The AIP-SSM, without any current signature state, starts performing analysis in midstream for all streams without an issue. The only portion of data that is lost is signature state for those flows in progress. The possible exposure is limited to an attacker being able to force a failover event. If an attacker can do this, they can cause a complete DoS by bringing down both active and passive firewalls. Configuration of the AIP-SSMs should be as close as possible to each other as they will perform the same job. Things like signature config, virtual sensor setup, filters, and overrides should all be similar, if not exactly the same. This helps to ensure that their behavior is the same.

Failover Pair in Active-Active Situation

The next scenario is much more complex, and involves a Cisco ASA failover pair deployed into an active/active asymmetric situation (Figure 3).

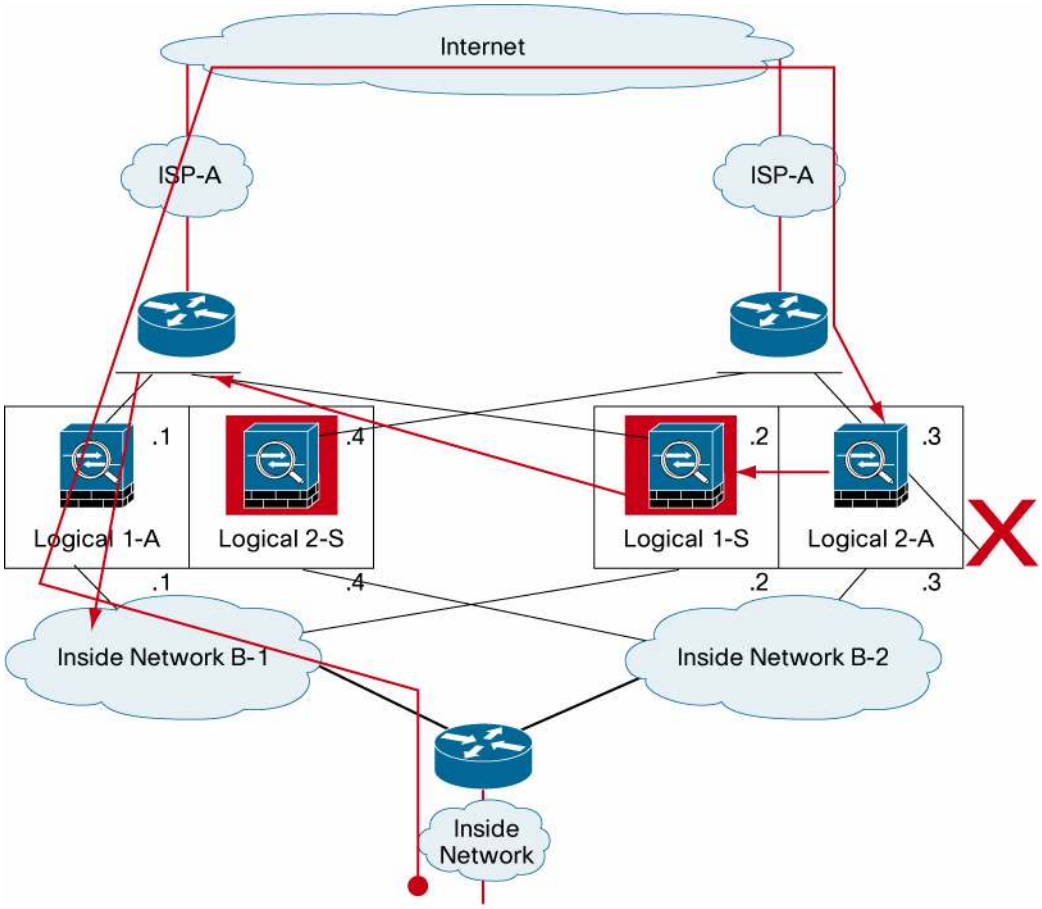
Figure 3. Failover Pair in Active-Active Deployment



In this deployment, because traffic can leave the network using network A-1 and come back using network A-2, different physical Cisco ASA appliances are involved in the primary packet path. To solve this issue, the appliance should be configured using active-active asymmetric routing mode. This deployment involves building two contexts on each Cisco ASA appliance, where context 1 on Cisco ASA 1 is the active context for network A-1 and context 2 on Cisco ASA 1 is the passive

context for network A-2. The opposite setup is done for Cisco ASA 2. Packet flow then looks like Figure 4.

Figure 4. Packet Flow



Since each appliance context pair only handles traffic that it is primary for, each appliance context's state tables are kept synchronized and up to date. None of this really matters to the AIP-SSM because even in this deployment, the AIP configuration portion is relatively easy. Once the modules are inserted and initialized, an important decision needs to be made as to whether one or two virtual sensor policies should be created and used due to the fact that the Cisco ASA appliances are using multiple virtual contexts. If one policy is desired, all packets from both contexts on the appliance will be sent to that same virtual sensor. If multiple virtual sensors are created, the packets from each context can go to their own virtual sensor for analysis. If the decision is made to create multiple virtual sensor "policies" on one AIP-SSM, a similar configuration should be created on the other AIP-SSM to match/mirror the configuration of the other AIP-SSM. Other than virtual sensor creation decisions, the rest of the configuration is fairly straightforward. From the AIP-SSM's standpoint, this deployment is no different from the active-passive in that all packets for a flow traverse the same appliance and context, so complete flow visibility is maintained. If a failover event occurs, session state is maintained by the appliance and new and ongoing sessions get passed to the "backup" AIP-SSM without issue. That AIP-SSM starts analysis of the flows as it sees them.

Summary

The Cisco ASA AIP-SSM is a fully functional firewall and IPS solution that can be deployed in symmetric or asymmetric mode and supports stateful failover deployments. In either deployment mode, session state and evasion protection will be maintained because of advanced state features in the Cisco ASA operating system.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-459025-00 03/08

