ASA 8.2: Packet Flow through an ASA Firewall

Contents

Introduction

This document describes the packet flow through a Cisco Adaptive Security Appliance (ASA) firewall. It shows the Cisco ASA procedure to process internal packets. It also discusses the different possibilities where the packet could be dropped and different situations where the packet progresses ahead.

Prerequisites

Requirements

Cisco recommends that you have knowledge of Cisco 5500 Series ASAs.

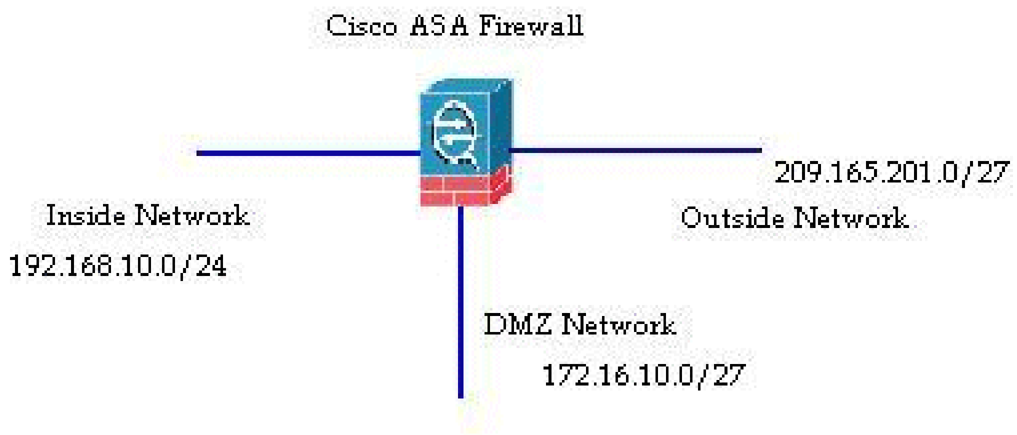
Components Used

The information in this document is based on Cisco ASA 5500 Series ASAs that run Software Version 8.2.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

The interface that receives the packet is called the **ingress** interface and the interface through which the packet exits is called the **egress** interface. When you refer to the packet flow through any device, the task is easily simplified if you look at it in terms of these two interfaces. Here is a sample scenario:



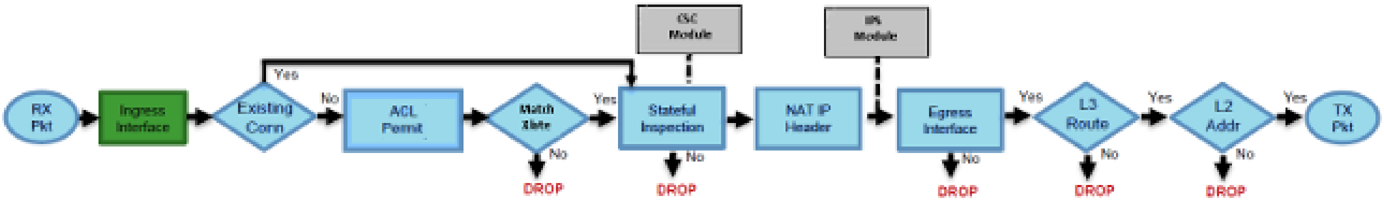
When an inside user (192.168.10.5) attempts to access a web server in the demilitarized zone (DMZ) network (172.16.10.5), the packet flow looks like this:

- Source address - 192.168.10.5
- Source port - 22966
- Destination address - 172.16.10.5
- Destination port - 8080
- Ingress interface - Inside
- Egress interface - DMZ
- Protocol used - TCP (Transmission Control Protocol)

After you determine the details of the packet flow as described here, it is easy to isolate the issue to this specific connection entry.

Cisco ASA Packet Process Algorithm

Here is a diagram of how the Cisco ASA processes the packet that it receives:



Here are the individual steps in detail:

1. The packet is reached at the ingress interface.
2. Once the packet reaches the internal buffer of the interface, the input counter of the interface

is incremented by one.

3. Cisco ASA first looks at its internal connection table details in order to verify if this is a current connection. If the packet flow matches a current connection, then the Access Control List (ACL) check is bypassed and the packet is moved forward.If packet flow does not match a current connection, then the TCP state is verified. If it is a SYN packet or UDP (User Datagram Protocol) packet, then the connection counter is incremented by one and the packet is sent for an ACL check. If it is not a SYN packet, the packet is dropped and the event is logged.
4. The packet is processed as per the interface ACLs. It is verified in sequential order of the ACL entries and if it matches any of the ACL entries, it moves forward. Otherwise, the packet is dropped and the information is logged. The ACL hit count is incremented by one when the packet matches the ACL entry.
5. The packet is verified for the translation rules. If a packet passes through this check, then a connection entry is created for this flow and the packet moves forward. Otherwise, the packet is dropped and the information is logged.
6. The packet is subjected to an Inspection Check. This inspection verifies whether or not this specific packet flow is in compliance with the protocol. Cisco ASA has a built-in inspection engine that inspects each connection as per its pre-defined set of application-level functionality. If it passed the inspection, it is moved forward. Otherwise, the packet is dropped and the information is logged.Additional security checks will be implemented if a Content Security (CSC) module is involved.
7. The IP header information is translated as per the Network Address Translation/ Port Address Translation (NAT/PAT) rule and checksums are updated accordingly. The packet is forwarded to Advanced Inspection and Prevention Security Services Module (AIP-SSM) for IPS related security checks when the AIP module is involved.
8. The packet is forwarded to the egress interface based on the translation rules. If no egress interface is specified in the translation rule, then the destination interface is decided based on the global route lookup.
9. On the egress interface, the interface route lookup is performed. Remember, the egress interface is determined by the translation rule that takes the priority.
10. Once a Layer 3 route has been found and the next hop identified, Layer 2 resolution is performed. The Layer 2 rewrite of the MAC header happens at this stage.
11. The packet is transmitted on the wire, and interface counters increment on the egress interface.

Explanation of NAT

Refer to these documents for more details on the order of NAT operation:

- Cisco ASA Software Version 8.2 and earlier
- Cisco ASA Software Version 8.3 and later

Show Commands

Here are some useful commands that help track the packet flow details at different stages in the process:

```
show interface
show conn
show access-list
show xlate
show service-policy inspect
show run static
show run nat
show run global
show nat
show route
show arp
```

Syslog Messages

Syslog messages provide useful information about packet processing. Here are some example syslog messages for your reference:

- Syslog message when there is no connection entry:`%ASA-6-106015: Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on interface interface_name`
- Syslog message when the packet is denied by an ACL:`%ASA-4-106023: Deny protocol src [interface_name:source_address/source_port] dst interface_name:dest_address/dest_port by access_group acl_ID`
- Syslog message when there is no translation rule found:`%ASA-3-305005: No translation group found for protocol src interface_name: source_address/source_port dst interface_name:dest_address/dest_port`
- Syslog message when a packet is denied by Security Inspection:`%ASA-4-405104: H225 message received from outside_address/outside_port to inside_address/inside_port before SETUP`
- Syslog message when there is no route information:`%ASA-6-110003: Routing failed to locate next-hop for protocol from src interface:src IP/src port to dest interface:dest IP/dest port`

For a complete list of all syslog messages generated by the Cisco ASA along with a brief explanation, refer to the Cisco ASA Series Syslog Messages.

Related Information

- **Cisco ASA Support Page**
- **Cisco ASA 5500 Series Command Reference, 8.2**
- **Cisco ASA 5500 Series Configuration Guide, 8.3**
- **Technical Support & Documentation - Cisco Systems**