

Perimeter Router Security

[Jolts]



Aditya Sood
Handle : ZeroKnock

Zknk Den

Topic Designed As:

- 0x01] Cisco Express Forwarding.
- 0x02] Unicast Reverse Path Forwarding.
- 0x03] TCP Intercept.
- 0x04] Network Address Translation.
- 0x05] Committed Access Rate.
- 0x06] Logging.
- 0x07] Conclusion.

Abstract:

When one connect its enterprise network to internet ,one is connecting its network to the thousands of network that are unknown thus giving millions of people an opportunity to access your assets. As such it leads to information sharing as the assets are being used by various people in the different organizations and places. This Paper describes the Technologies that are used to minimize the threat of potential intruders to the enterprise and its assets.

0x01]Cisco Express Forwarding:

-[]- It is an advanced layer 3 topology based forwarding mechanism that optimizes the network performance and accommodates the traffic characteristics of the internet for the IP protocol.

-[]- A CEF table is designed having the entries same as router table which is further based on the Forward Information Base(FIB) to make destination based switching decisions. CEF else creates a adjacency table which maintain layer 2 next hop addresses.

-[]- CEF operates in two different mode central and distributed.In central mode the FIB and adjacency table reside in the router processor and router processor performs the forwarding.

-[]- Distributed mode comes into play where there are inbuilt processors.In Distributed mode switching decisions are made through Router Line cards.

This technology is playing a crucial role in enterprise security.

0x02]Unicast Reverse Path Forwarding:

-[]- It is a technology driven feature used to prevent problems caused by packets with forged IP sources addresses passing through the router.

-[]- It requires CEF switching mechanism to be enabled globally on the router.Unicast RPF searches through the FIB using the packets source IP addresses.

-[]- The effect of Unicast RPF is that packets with the forged IP addresses will be dropped by the router and will not be forwarded beyond routers ingress interface.

Jolts:

-[]- Cisco Express Forwarding must be enabled for unicast Reverse Path forwarding.

-[]-Unicast RPF helps to prevent denial-of-service attacks.

0x03]TCP Intercept:

TCP Intercept is a software feature design to combat the denial- of service attacks mainly SYN flooding.As we know TCP protocol uses three way handshake for establishing end-to-end connection before data is allowed to flow.

SYN Attack:

A SYN attack occurs when attacker exploits the buffer space a networked device uses during TCP session initialization handshake.The attacker sends large amount of data with SYN bit set to the target host.Hence resources get exhausted waiting for the response.The target host eventually times out while waiting for the proper response.

TCP Intercept is designed to combat SYN flooding DoS attack by:

- 1) Tracking.
- 2) Intercepting.
- 3) Validating.

TCP works in three different modes:

Intercept mode:

In this software intercepts every single incoming request.

Watch mode:

Connections are allowed to pass through routers to the servers but watched passively until they are established.

Aggressive mode:

This mode comes to play when the system is under attack.when number of connections exceed 1100.

Jolts:

Firewall is first and last line of defense for security related issues

0x04]Network Address Translation:

Cisco has implemented a feature known as Network Address Translation.It tells the way to use IP addresses in multiple internetworks by replacing original source or destination IP addresses in IP packets.The basic functionality is that maintaining a connection of private networks to the public networks sustaining with full security reducing the IP depletion problem.

In this when the host inside the private network sends a packet through NAT router the private addresses are converted to registered globally routed IP addresses.

NAT automatically creates a makeshift firewall between the internal trusted network and the outer trusted network.

NAT uses different types of IP Addresses:-

- 1) **Inside Local IP Address.**
- 2) **Inside Global IP Address.**
- 3) **Outside Global IP Address.**
- 4) **Outside Local IP Address.**

NAT uses two types of address translation simple and extended. Port Address Translation is also a variant of NAT. NAT increases the flexibility between various networks. It provides an ample security to the private networks inside organizations

0x05]Committed Access Rate:

Committed Access Rate is a software feature that implements both classification of services and policing of traffic through rate limiting i.e. limiting the input or output transmission of an interface based on configurable set of criteria.

CAR uses bucket measuring system. Tokens are inserted into bucket at the committed rate and number of tokens in the bucket is limited by the configured burst size. Action is confirmed when the tokens match. Tokens are removed for one single action to get executed.

Token Bucket is a culmination of three components:

- 1) **Mean Rate (CIR) :-Average rate on which transmission occurs**
- 2) **Burst Size (Bc) :-Amount of data to be sent per time interval.**
- 3) **TimeInterval (Tc) :-Measurement of Bc/CIR**

Actions that are taken on the availability of tokens:

- 1) **Transmit**
- 2) **Drop**
- 3) **Set precedence then transmit.**
- 4) **Continue.**
- 5) **Set precedence and then continue.**

Jolts:

A Security administrator can use CAR's rate limiting feature to control maximum rate at which traffic is sent or received during times the router is receiving a stream of DoS attack packets.

0x06] Logging:

Logging of events that takeplace on the perimeter routers provides a security administrator with clear audit trail of each and every bit of information that traverses the router. This information is needed in order to assess the network activity and find out if network policies are functioning as it is designed.

Cisco Routers define certain levels of message logging and each level is based on the severity of the events.

Table:-

Debugging	-----	7
Informational	-----	6
Notifications	-----	5
Warnings	-----	4
Errors	-----	3
Critical	-----	2
Alerts	-----	1
Emergency	-----	0

The message are logged based on the defined codes.

Conclusion:

A breach in the integrity of enterprise network can be extremely costly and can open doors for multi faceted attacks on the system. These defined technologies are here to combat the attacks.