128T DOS/DDOS, IPS/IDS (DDII)

ABSTRACT

This whitepaper describes how 128T Session Based Router protect the network against well known Denial of Service (DOS) and Distributed Denial Of Service (DDOS) attacks. This paper also explains how 128T routers can Service Function Chain (SFC) with an existing Next Generation Firewall (NGFW) to provide Layer 5 through Layer 7 Application level firewall protection. Please note that, in this paper, we are referring combination of DOS, DDOS, IDS and IPS protection mechanism as DDII protection mechanism.

INTRODUCTION

DOS and DDOS are classes of attacks which attempt to make machines or network resources unavailable to legitimate users by overwhelming them with traffic from multiple sources. This poses a major threat to day-to-day business operations, and has successfully crippled many data networks. There are two different categories of network based DDOS attacks:

- Volume based DDOS attack: In this attack, the attacker typically floods the victim with high volume of packets or connections, overwhelming the network equipment and servers.
- Low-rate DOS attacks: These kind of attacks take advantage of the application implementation and design flaws.

Intrusion Detection Systems (IDS) are designed to detect malicious activities and Enterprise policy violations and report them. The detected activities are typically reported to the administrator through syslogs, alarms or are collected centrally using Security Information and Event Management (SIEM) systems. IDS systems can detect several attacks which are usually classified as either signature based or anamoly based attacks. Signature based IDS referes to the detection of attacks by looking for specific pattern in the packet, such as specific byte of sequence in network traffic. Anamoly based attacks are used to detect unknown attacks. The usual procedure followed in the anamoly based attacks detection is to compare the current network activity with the trustworthy activity and detect any malicious behavior. Since IDS provides deep visibility into network activity, it can also be used to help pinpoint problems with an Enterprise's security policy, document existing threats, and discourage users from violating these policies.

At the basic premise, Intrusion Prevention Systems (IPS) have all the features of an IDS system, but can also stop the malicious traffic from bringing down entire Enterprise network. IPS sytems typically sits inline with the traffic flow on a network, actively analyzing the live traffic to detect and prevent attacks. IPS systems usually stops attacks by terminating the network connections and associated user sessions causing the attack, by blocking access to the target from the user account, blocking IP address, or other attribute associated with that attacker. IPS systems are very useful to detect and prevent attacks like DoS/DDoS attacks, brute force attacks, vulnerability detection, protocol anomaly detection and prevention of zero day unknown attacks.

128T Session based Networking platform provides a native Zero Trust Security (ZTS) and Hyper-segmented network architecture allowing organization to achieve and exceede Layer 3/Layer4 DDII compliance requirements. Also, 128T solution integrates multiple middle-box functionalities (security, routing, firewall, VPN and Load balancer) into a single platform thus simplifying the overall network architecture while minimizing the cost and time to build a true secure network.

Given the session based nature of 128T platform and with support for SVR, Hypersegmentation, Deny-by-Default policy and with Zero Trust Security (ZTS) network architecture, 128T eliminates most of the Layer 3/Layer 4 DDII attacks. Additionally, 128T supports static and dynamic Service Function Chain (SFC) to allow an Enterprise to SFC with layer 5-7 Next Generation Firewalls (NGFW) to provide additional security.

Unlike a perimeter based firewall where in DDII protection is applied at the edge/perimeter of the network, 128T applies DDII protection to every session passing through the 128T routers irrespective of the location of the router in the network. Also, the context specific nature of 128T allows it to provide better analytics and syslogs to track and discover these attacks.

128T SESSION BASED NETWORKING PLATFORM

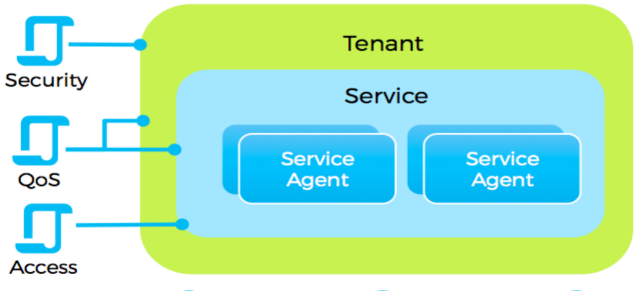
128T Session based Networking Platform (router) innovatively combines routing and security under one platform. Security is the DNA of the 128T Session based router and every aspect of this product is built with keeping security as the central focus.

Some of the key features applicable to the DDII protection on 128T platform include:

Service centric Tenant based Security architecture

The traffic in 128T platform is processed, routed, and controlled in a service-centric manner. Therefore services make up a fundamental building block for the operation of the 128T router.

Services can be made to model a given application, reachable at a given address, set of addresses, or subnets.

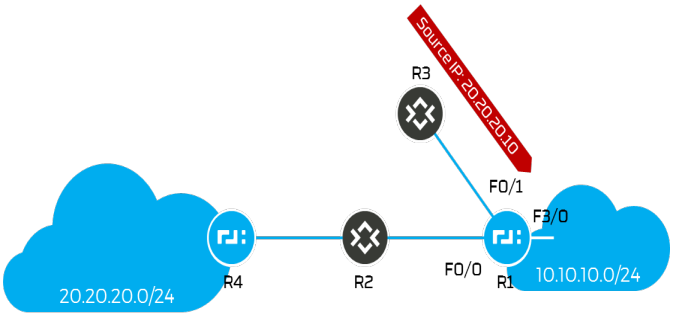


A tenant functions as a network partition used to group services together. As sessions are processed through the 128T solution, the tenant becomes an important construct for route determination, segmentation, classification, policy, and many other capabilities.

128T provides the unique capability to specify security policy, Quality of Service (QOS) parameters, and access control policies on per service per tenant basis. This means, it is possible to have unique encryption/authentication keys, custom traffic engineering parameters and tight access control per service per tenant basis thus providing a flexible way to **segment** and isolate the traffic and apply different traffic profiles on a per service per Tenant basis.

URPF Spoof Prevention

When connected to public networks, one common method to initiate an attack is to utilize IP source address spoofing. The hacker attempts to send traffic into the network with a source address that is known or trusted by the target. If no protection exists, the organizational network will allow the traffic and potentially be open to a number of different attack types. Several well known attacks take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks. With Unicast Reverse Path Forwarding (URPF) check, all traffic that comes into a configured interface is checked to ensure that the interface that would be used to route traffic back to the source address is the same interface that was used to receive the traffic.



For example, assume a branch connected to a data center using 128T routers as shown in figure. The correct path to the 10.10.10.0 branch to the 20.20.20.0 data center is through R2 and R4. If uRPF Strict Mode is configured on R1's F0/0 and F0/1 interfaces, traffic to and from the 10.10.10.0 and 20.20.20.0 network would be allowed, as long as it was received on the F0/0 interface. If an attacker attempted to send traffic to the 10.10.10.0 network through R3 using a source address of 20.20.20.10 without uRPF enabled, traffic could pass through and reach the destination. With uRPF enabled, the device (in this case R1) will check if the "best" return path is using the F0/1 interface where the traffic was

received; when the “best” return path is shown to be through the F0/0 interface the uRPF check will fail and the traffic will be dropped.

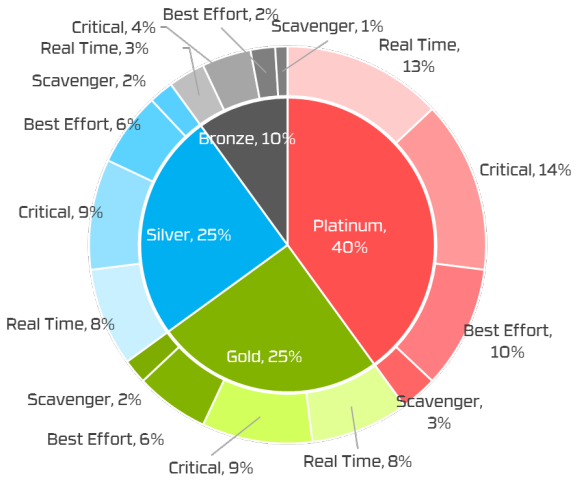
Quality of Service (QOS)

The 128T solution delivers guaranteed and differentiated services on any IP network to allow fine control of traffic at the service level. Secure Vector Routing brings context awareness to the network by associating transient sessions. This enables centralized management, granular control, individualized flows, infused security, and dynamic traffic management. It also enables the ability to provide granular and unsurpassed quality of service offerings.

Within a 128T router, the Quality of Service (QoS) toolset will offer many functions. The 128T router will be able to offer differentiated services based on a class model. Combined with intelligent path selection, fast failover, prioritization, shaping, duplication, and error correction across the network, this QoS toolset will bring best in class quality of experience to end-user applications.

Traffic Classes

The 128T solution supports a 4x4 class model. This makes a total of 16 different classes arranged in a 2 level hierarchy to provide unlimited possibilities for classification, policing, and queuing. according to the business needs of the organization. An enterprise can map traffic within their network according to application types (as shown in figure on the left) or a SD-WAN service provider can choose to provide traffic classes based on customer’s served (as shown in figure on the right).

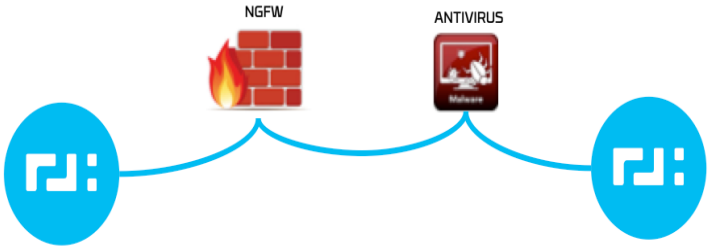


The solution enables granular control of bandwidth, priorities, and weights associated with each traffic class. In the event of network congestion, these parameters ensure that application requirements for different SLAs are honored. This ensures a superior end-user experience.

The 128T router can be operated in different trust modes to ensure that the administrator is in complete control of the overall service offering and can curb any flow trying to game the system and attack the network. Intelligent session identification ensures superior experience to the end user.

Service Function Chain (SFC)

128T is built on the principle that *security is not a stand-alone function* and should be present and enforced at every point in the network. Our approach is to not to supplement the existing routed networks with yet another third party middle-box that grafts security into an insecure network, but to replace the routing plane with one built from the ground up with security principles at its core. 128T has inbuilt capability to support service functions like Layer 3/Layer 4 stateful Firewall, Load Balancing and VPN technology which can easily replace standalone devices in the market at a fraction of the cost while providing better security and network segmentation.



With virtualization of network functions with Network Function Virtualization (NFV), more and more network service functions (SF) are virtualized and are run on COTS platform. Running SF on COTS platform allows Enterprise and Service providers to Service Function Chain (SFC) these functions to build a network. For example, in a cloud CE deployment, you could deploy all the service functions on the cloud and deploy a dumb CPE device in the branch and have the dumb CPE device tunnel all the packets to the cloud to apply service functions like firewall, DPI and so on. This allows the customer to simplify the branch deployment and eliminate the need for building and deploying a smart and custom built CPE device to every branch and end user customers.

In addition to supporting in built service functions, 128T can Service Function Chain (SFC) with standalone service functions (like Next Generation Firewall and Load Balancer) from other vendors. 128T support both static and dynamic SFC. 128T can support dynamic SFC using the IETF draft Network Service Header (NSH[1]) protocol. Networks with a Network Function Virtualization (NFV) strategy can utilize 128T router for core networking and security and then add on layer 5 and above firewalls from companies like Palo Alto, proxies, WAN optimizers, and additional functions.

[1] https://datatracker.ietf.org/doc/draft-quinn-sfc-nsh/

DOS AND DDOS ATTACK PREVENTION THROUGH 128T PLATFORM

128T provides finer controls at the session and service level to limit and eliminate volume based and low-rate DDOS attacks. Some of the controls provided to limit these attacks include:

- Limiting the session establishment rate per service agent
- Limiting the number of sessions per service agent
- Restricting per-flow bandwidth rates per traffic service class
- Restricting per-flow burst rates per traffic service class
- Enforcing inactivity timeouts per session type

The above controls eliminate most of the application layer bandwidth saturating flooding and Non-malicious/un-intentional DDII attacks. In addition to the above controls, 128T takes specific steps to protect against well known DDII attacks as described in the following sections.

128T also generates appropriate security events in the form of alarms, syslogs and auditlogs when an attack is detected or prevented. 128T will automatically tune the dampening of the security event generation when same type of attack is repeatedly detected/prevented to eliminate overwhelming of the 128T system as well as to prevent over loading the SIEM.

128T and ICMP attack prevention

ICMP FLOODING

This is similar to the UDP attack, where the attacker overwhelms the network with ICMP packets (for example, ping packets).

The 128T system mitigates this attack by:

- Unicast Reverse Path Forwarding for source address in ICMP
- Limiting the number of concurrent ICMP replies
- Disabling IP directed broadcast so that the ICMP request is not forwarded to all clients in the network

ICMP TUNNELING

In this attack, the attacker sets up a covert tunnel between the sender and receiver for tunneling rogue traffic.

128T mitigates this attack by limiting the packet size of the ICMP packets. In a normal ICMP echo request, the packet length will be 42 bytes, where the data length is 0, and if we append any data in to the ICMP data field then the size of the packet will increase. So, if data is present in the ICMP echo request, 128T will drop those packets and alert the administrator.

SMURF ATTACK

With URPF support and with abilility to black hole/drop ICMP response message, 128T will protect the network against SMURF[2] attack.

FRAGILE ATTACK

Fragile attack is same as SMURF attack but by making use of UDP packets instead of ICMP packets. With support for URPF and with ability not to respond to broadcast addresses, 128T will protect the network against Fragile attack.

INFORMATION GATHERING ATTACK

Under the information gathering attack, one can use different methods within the ICMP to find out live host, network topology, OS fingerprinting, ACL detection, and so on. A well known way to discover hosts on the network is to send an ICMP echo request (type 8) which should prompt target hosts to respond with ICMP echo reply messages.

128T will drop all ICMP packets by default, the only way to enable ICMP to pass through an 128T system is to explicitly create a service under a tenant to allow ICMP. So, this attack can be blocked in a fine-grained way per service on the 128T platform.

TRACEROUTE ATTACK

In this attack traceroute is used for gathering network topology[3]. As said before, unless explicitly enabled as a service under a tenant, 128T will drop all ICMP packets. When ICMP is enabled as a service, 128T will drop ICMP packets with low TTL. Once this attack is detected, 128T will alarm the administrator on this attack and will block the source of this attack for a pre-configured interval of time.

PORT SCAN ATTACK

Port scan is usually performed by sending TCP or UDP packets to detect open ports[4] and scanner relies on the ICMP failure respnse to detect open ports. 128T has the default policy of “deny-by-default” which means unless a service is configured for a specific port, packets will be silently dropped without a response. In addition to this, 128T keep track of ICMP failures

---

[2] https://en.wikipedia.org/wiki/Smurf_attack

[3] http://resources.infosecinstitute.com/icmp-attacks/#gref

[4] https://nmap.org/book/man-port-scanning-techniques.html

messages going to the same source address. If the ICMP failure message per source crosses a configured threshold, 128T will raise an alarm and block the source for the configured interval.

OS FINGERPRINTING

Fingerprinting is a technique to find out what OS the server is running. In this attack, the attacker typically relies on the Time To Live (TTL) value in the ICMP message. In most of the cases, If the TTL value is 128, it means the response is coming from a Windows based machine and if the TTL value is 64, the response is coming from a Linux machine. 128T eliminates this attack by always returning the same TTL value in the ICMP response message.

ICMP ROUTE DISCOVERY

The ICMP router discovery protocol will discover the IP address of the neighbouring routers. The ICMP router discovery messages are called “Router Advertisements” [ICMP message type 9] or “Router Solicitations” [ICMP message type 10]. ICMP router discovery enables hosts to discover the existence of a neighbouring routers. Given the absence of any form of authentication attached to these messages, it is impossible for a host to say whether the received message is a legitimate message or not. Due to the above issue, an attacker can perform a man in the middle attack where in an attacker will act as middle man for all the communication from the source to the endpoint. Attackers can also spoof ICMP router discovery messages and remotely add bad route entries into a victim’s routing table.

128T completely eliminates this attack by blocking ICMP message types 9 and 10.

ICMP SOURCE QUENCH ATTACK

An ICMP source quench message (ICMP type 4, code 0) is designed to be issued when a router is unable to handle the volume of packets coming in. It is a request for the sender to lower the volume of incoming traffic.

128T protects the network against this attack by blocking all the ICMP source quench messages.

ICMP MASK REQUEST ATTACK

In this attack, an attacker sends an ICMP Type 17 Address Mask Request to gather information about a target's networking configuration. An Address Mask Request is an ICMP type 17 message that triggers a remote system to respond with a list of its related subnets, as well as its default gateway and broadcast address via an ICMP type 18 Address Mask Reply datagram. Gathering this type of information helps an attacker plan router-based attacks as well as denial-of-service attacks against the broadcast address.

128T protects the network agains this attack by blocking all ICMP type 17 and type 18 messages.

ICMP LARGE PACKET/PING OF DEATH/SSPING ATTACK[5]

128T protects the network from this attack by blocking large ICMP packets.

ICMP FLOOD/PING FLOOD

A **ping flood** is a simple denial-of-service attack where the attacker overwhelms the victim with ICMP "echo request" (ping) packets. This is most effective by using the flood option of ping which sends ICMP packets as fast as possible without waiting for replies.

128T will drop all ICMP packets by default, the only way to enable ICMP to pass through an 128T system is to explicitly create a service under a tenant to allow ICMP. Administrator can rate control the traffic per service and by configuring a very low rate for ICMP service, administrator can completely eliminate this attack.

ICMP TRASH/ICMP ERROR PACKET FLOOD[6]

By default, 128T routers does not respond back with the ICMP error packets for ports which are unreachable on 128T routers. Also, by default, all the ICMP error packets traversing through 128T routers will be dropped.

ICMP SPOOFED UNREACHABLE FLOOD ("SMACK/BLOOP/PUKE") ATTACK[7]

By default, 128T routers does not respond back with the ICMP error packets for ports which are unreachable on 128T routers. Also, by default, all the ICMP error packets traversing through 128T routers will be dropped.

128T and IP attack prevention

UNKNOWN PROTOCOL

128T routers drop all the unknown protocol packets.

---

[5] https://en.wikipedia.org/wiki/Smurf_attack

[6] https://en.wikipedia.org/wiki/UDP_flood_attack

[7] https://en.wikipedia.org/wiki/UDP_flood_attack

TEARDROP ATTACK

Teardrop attacker makes use of overlapping IP fragments to launch this attack. When IP packets are larger than the network MTU, IP packets are broken up into smaller fragments, with each fragment having the original IP packet's header, and field that tells the TCP/IP stack what bytes it contains. The packet is fragmented and is sent from the source to destination. In the destination point, the fragments need to be put back together again. What happens with teardrop though is that the IP fragments will have overlapping fields. When the destination tries to reassemble them, it cannot do it, and if it does not know to combine these packet fragments out, it can quickly fail and possible crash the system.

128T handles fragmented packets in a smart way and special care is taken to make sure that the offsets within the IP fragments are valid.

IP STREAM OPTION

Hackers who initiate IP stream option attack commonly send large number of IP packets with IP options enabled. For hardwar based routers, usually, when they get packets with IP options, packets take the slow path and are handled in software. This significantly reduces the total throughput of the router.

Since 128T router is completely software based and since it makes use of the Intel's high performance data plane, packets with and without IP options are handled in a similar fashion,

IP SPOOFING[8]

SVR capability along with URPF functionality, 128T completely eliminate this attack.

IP SOURECE ROUTE OPTION, STRICT/IP SOURCE ROUTE OPTION, LOOSE

128T ignores any packet with IP source routing enabled thus completely eliminating this attack.

IP HEADER ATTACKS

There are classes of attacks which focuses on manipulating IP header. These attacks include (but not limited to):

- IP short header attack
- IP Malformed packet attack
- IP Bad Option attack

---

[8] https://en.wikipedia.org/wiki/IP_address_spoofing

128T drops any IP packet without a legitimate IP header thus completely eliminating this attack.

BANANA & LAND ATTACKS

Both of these attacks rely on replaying the packet back to the client who sent the packet. By default, 128T system has mechanism built to make sure that the packets are not sent back to the originator of the packet. Also, 128T has a built in loop prevention mechanism in the metadata wherein 128T router includes a unique router id to identify every 128T router the packet has traversed. If 128T detects duplicates router id in the metadata, the packet will be immediately dropped.

PEER-TO-PEER ATTACKS

Because of Hyper-segmentation and zero trust architecture of 128T system, 128T minimizes the possibility of launching a peer-to-peer attack[9]. Hyper-segmentation allows sessions to be classified under tenants and services and only members belonging to a tenant are allowed to access services within a tenant. Also, the concept of tenant and services extend throughout the domain of the Authority thus providing hyper-segmentation across the network.

IP FRAGMENT ATTACK

There are classes of attacks which focuses on manipulating IP fragments. These attacks include (but not limited to):

- IP Fragmnt Overlap
- IP Fragment Buffer Full
- IP Fragment Overrun
- IP Frament too many datagrams
- IP Fragment incomplete datagram
- IP Fragment too small

128T eliminates all the IP fragment related attacks by:

- Validating the offsets with the fragment to be legimite before processing the fragment
- Validate that the total size of the fragment does not exceed the max IP packet size
- Keep enough room in the fragment buffer space by timing out old fragments
- Detect and drop small fragments
- Rate limit fragment per sessions to make sure that it does overwhelm the router.

---

[9] https://en.wikipedia.org/wiki/Denial-of-service_attack#Peer-to-peer_attacks

128T and TCP attack prevention

TCP HEADER MANIPULATION ATTACKS

These are classes of attacks which focuses on manipulating TCP packets. These attacks include (but not limited to):

- TCP sequence number attack[10] : 128T prevents this attack by making use of SVR and URPF technology.
- TCP reset attack: 128T prevents this attack by making use of SVR and URPF technology.

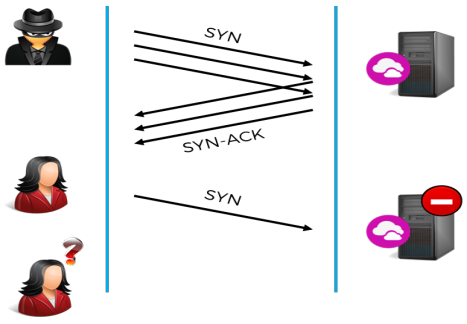
TCP HEADER MANIPULATION ATTACKS

Following TCP attacks focuses on manipulating the flags within the TCP header in attacking the system. 128T prevents these TCP attacks by dropping TCP packets which does not strictly follow TCP RFC.

- TCP packet without Flag
- TCP packets, oversized
- TCP FIN bit with no ACK bit set
- TCP packet with URG/OOB flag set (Nuke attack)
- TCP packet with SYN and FIN bit set

TCP SYN ATTACK

A SYN Flood is a form of DoS attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough resources to make the system unresponsive to legitimate traffic.



SYN Flood Attack

A SYN flood attack works by not responding to the server with the expected ACK code. The malicious client can either simply not send the expected ACK, or by spoofing the source IP address in the SYN, causing the server to send the SYN-ACK to a falsified IP address - which will not send an ACK because it never sent a SYN.

128T prevents SYN flood attack by:

[10] http://www.thegeekstuff.com/2012/01/tcp-sequence-number-attacks/

1. Enabling URPF support on all the interfaces to eliminate IP spoofing
2. Using the options mentioned in the RFC 4987 to protect agains SYN flood attack.

TCP SPLIT HANDSHAKE ATTACK[11]

This attack attempts to confuse the firewall into allowing traffic to pass from one network segment to another. The TCP split handshake blends features of both the three-way handshake and the simultaneous-open connection. The result is a TCP spoof attack that allows an attacker to bypass the firewall by instructing the target to "initiate"the session back to the attacker. Given the fact that SVR technology does not allow TCP handshake to complete without thorough inspection of the packet, this attack is impossible with 128T routers.

128T and UDP attack prevention

UDP FLOODING

This attack involves sending a large number of UDP packets to random destination ports. Since UDP is not session-oriented at the transport layer and does not use a handshaking technique like TCP, it is more difficult to mitigate such attacks.

The 128T mitigates UDP flooding using several techniques, in combination:

- Unicast Reverse Path Forwarding (URPF): Traffic will be accepted only if packets are received on the same interface on which the response is sent and the source IP address is reachable (present in the routing table)
- Through configuration, by blocking/limiting access to administrative ports from external access
- Maintaining a whitelist of UDP ports.
- Actively monitoring the traffic patterns proactively to detect and block traffic anomalies.

UDP HEADER MANIPULATION ATTACKS

There are classes of attacks which focuses on manipulating UDP packets. These attacks include (but not limited to):

- UDP short header attack: Packets with short UDP headers are automatically dropped by 128T routers.
- UDP Flood: 128T routers are protecting agains the UDP flood by SVR and URPF capabilities.
- UDP Spoofed Broadcast echo (Fragile attack): 128T routers are protecting agains the UDP flood by SVR and URPF capabilities.

---

[11] https://www.secplicity.org/2011/04/15/what-is-the-tcp-split-handshake-attack-and-does-it-affect-me/

- UDP Bomb attack: To launch this attack, the attacker sends UDP packets by setting the length field in the UDP packets less than the length derived from the IP header. 128T prevents this attack by validating the length field to make sure that it is legitimate.

UDP ATTACK ON DIAG PORTS (PEPSI ATTACK)

UDP is a connectionless protocol that doesn't use a handshake mechanism to establish a connection. This makes it relatively easy to abuse for flood attacks. A common type of UDP flood attack often referred to as a ***Pepsi attack***, is an attack in which the attacker sends a large number of forged UDP packets to random diagnostic ports on a target host. The CPU time, memory, and bandwidth required to process these packets may cause the target to become unavailable for legitimate users.

By default, all the UDP ports are disabled on 128T routers. The only way to enable UDP ports is by creating a service corresponding to the UDP ports. Given the fact that every service defined on 128T strictly follows DOS and DDOS prevention, launching this attack on 128T router is impossible.

128T and DNS attack prevention

DNS AMPLIFICATION

In this attack, DNS requests are sent with the RD (Recursion Desired) flag set which causes DNS servers to forward the requests to other DNS servers. Since these servers accept request from any source, this can lead to a high volume of spoofed traffic and even more traffic outbound if the request finds a hit. The attacker can also create a **SMURF**[12] attack by spoofing the source IP of a victim.

The 128T system mitigates this attack by:

- Unicast Reverse Path Forwarding for source address in DNS
- The threshold of DNS traffic (by volume) that traverses the 128T domain will be limited by configuration.

[12] https://en.wikipedia.org/wiki/Smurf_attack

128T and SSL attack prevention

SSL/TLS DDOS ATTACKS

Encrypted DDOS attacks are becoming more prevalent since it allows the attacker gain the advantage of consume more resource for processing the handshake messages and performing encryption and decryption.

The 128T system mitigates this attack by:

- Limiting the session establishment rate per service agent
- Limiting the number of sessions per service agent
- Restricting per-flow bandwidth rates per traffic service class
- Restricting per-flow burst rates per traffic service class
- Limiting the number of SSL connections per source IP address

SUMMARY

128T Session based routers is the only platform in the Industry which provides true ZTS, session based hyper-segmentation, fine grained QOS, Secure Vector Routing and a “deny-by-default” policy allowing organization to achieve and exceede Layer 3 /Layer 4 DDII requirements. 128T overcomes the deficiencies of perimeter based security by providing security, firewall, IDP, DOS/DDOS control, traffic engineering, and access control at the individual session level. Given the fact that 128T solution integrates multiple middle-box functionalities (security, routing, firewall, VPN and Load balancer) into a single platform, the overall network architecture will be simplified while minimizing the cost and time to build a ZTS enabled network. With our software-defined, session-based and service-centric approach to routing, the 128T Networking Platform, delivers both Enterprises and Service Providers breakthrough results in end-to-end security, agility, cost and performance.