A10 THUNDER TPS

SECURITY TARGET

VERSION 1.2

NTT Com Security (Norway) AS - www.nordics.nttcomsecurity.com

Office address: Havnegaarden – Kystveien 14 – 4841 Arendal
Postal address: Postboks 721 Stoa – 4808 Arendal
T +47 37 01 94 00

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

Abbreviation	Description
ACK	Acknowledge character
ACOS	Advanced Core Operating System
API	Application Programming Interface
BGP	Border Gateway Protocol
CEF	Common Event Format
CLI	Command-line Interface
DDoS	Distributed Denial of Service
DPI	Deep Packet Inspection
FPGA	Field Programmable Gate Array
FTA	Flexible Traffic Acceleration
GUI	Graphical User Interface
PPS	Packets per second
REST	Representational State Transfer
SSD	Solid-State Drive
SSMP	Symmetric Scalable Multi-Core Processing
SYN	Synchronize
TPS	Threat Protection System

DEFINITIONS

Definition	Description
GLID	Applies a custom set of traffic rates

1. ST INTRODUCTION (ASE_INT)

1.1. ST AND TOE REFERENCES

The following table identifies the Security Target (ST).

Item	Identification
ST title	A10 Thunder TPS Security Target
ST version	1.2
ST author	NTT Com Security (Norway) AS

The following table identifies the Target Of Evaluation (TOE).

Item	Identification
TOE name	A10 Thunder TPS
TOE hardware version	Thunder 3030S TPS
TOE firmware version	3.2.2-P7

The following table identifies common references for the ST and the TOE.

Item	Identification
CC Version	3.1 Revision 5
Assurance level	EAL2 augmented with ALC_FLR.1
PP Identification	None

1.2. TOE OVERVIEW

The TOE is comprised of Thunder 3030S TPS, that provides high-speed monitoring and scrubbing of client-server traffic. A10 Thunder TPS (Threat Protection System) is built upon the Advanced Core Operating System (ACOS) platform, with Symmetric Scalable Multi-Core Processing (SSMP) software architecture for tracking of network flows.

A10 Thunder TPS provides network-wide protection against distributed denial of service (DDoS) attacks, thereby avoiding downtime caused by such attacks and enabling data center resources to be used productively. The system performs DDoS protection enforcement for service providers, Web site operators and enterprises, and enables service availability against volumetric, protocol, resource, and application-layer attacks. For handling large DDoS attacks, the system capacity offers 300 Gbps of inspection and throughput.

For A10 Thunder TPS, customized actions can be taken against application-layer attacks as needed with Berkeley Packet Filters and RegEx DPI matching technology. Further, A10 Thunder TPS models equipped with Field Programmable Gate Array (FPGA)-based Flexible Traffic Acceleration (FTA) technology detect and mitigate up to 60 common attack vectors in hardware, with no impact to performance. More complex application-layer attacks (TCP, UDP, DNS, HTTP, and SSL) are mitigated by a multi-core CPU complex based on Intel Xeon CPUs. For Thunder 3030S TPS, without the FPGA-based FTA technology, these same attack vectors are detected in in software by the CPU.

A10 Thunder TPS can be integrated into network architectures of different size, with flexible deployment models for in- and out-of-band operations, and routed or transparent operation modes. Such flexible DDoS Mitigation solution eases integration into various networking architectures.

A10 Thunder TPS is a family of high-performance appliances that detect and mitigate multi-vector DDoS attacks at the network edge, functioning as a first line of defense for a network infrastructure, and can be deployed in the following modes:

- Symmetric (client-to-server and server-to-client)

- Asymmetric (client-to-server only)
- Tap (log only)

A Thunder TPS device can run the feature in only one of these modes at any given time. However, these modes can be used in combination among multiple DDoS Mitigation peers. For example, running one of the peers in Tap mode configures the device to act as the master device for Black/White List synchronization. The figures 1-3 describe possible operation modes for deployment of A10 Thunder TPS in enterprise networks.

SYMMETRIC DEPLOYMENT

In a Symmetric deployment, the A10 Thunder TPS device is deployed in-line with client-server traffic. DDoS Mitigation can be applied to either or both traffic directions, client-to-server and server-to-client. See figure 1 for an example use of A10 Thunder TPS in a symmetric mode.

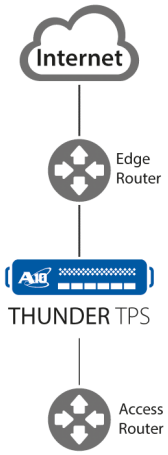

Figure 1: Symmetric mode

This mode provides continuous, comprehensive detection and mitigation, with more application-level attack mitigation options.

ASYMMETRIC DEPLOYMENT

In an Asymmetric deployment, the A10 Thunder TPS device is not in-line with client-server traffic. Instead, traffic is redirected to the Thunder TPS device when needed for scrubbing. See figure 2 for an example use of A10 Thunder TPS in an asymmetric mode.

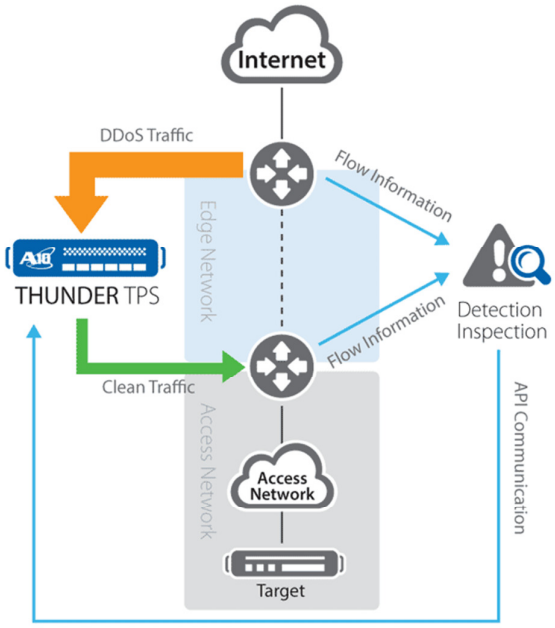

Figure 2: Asymmetric mode

This mode describes an on-demand, or permanent (proactive) volumetric mitigation, triggered manually or by flow analytical systems. With the aXAPI open RESTful API (Application Programming Interface), A10 Thunder TPS enables integration to a vendor custom or third-party detection solutions.

TAP DEPLOYMENT

Tap deployment is designed for operators who want high-speed DDoS detection visibility without mitigation. This is useful in scenarios where operators want to gather telemetry to formulate policy decisions or develop dynamic white lists / black lists and act as a "master" to other TPS devices.

In a Tap deployment, the Thunder TPS device is not in-line with client-server traffic. Traffic is mirrored by tap devices to the Thunder TPS device. Violations of DDoS Mitigation policy are logged but no production traffic is affected by the policy. See figure 3 for an example use of A10 Thunder TPS in a tap mode.

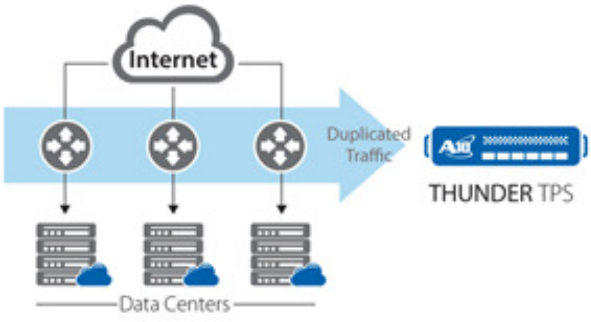

Figure 3: Tap mode

This mode enables deep traffic analysis, establishment of peacetime traffic baselines, establishing thresholds for attack detection, and creation of white/black lists that can be distributed to other Thunder TPS units. Tap mode deployment applies DDoS Mitigation to

traffic, but drops traffic that passes scrubbing, instead of sending it. Tap mode deployment is useful for testing DDoS protection features.

Asymmetric deployment and Tap deployment have been excluded from the Common Criteria evaluated configuration.

1.3. TOE DESCRIPTION

TOE scope for A10 Thunder TPS includes Thunder 3030S TPS. See Figure 4.

Figure 4: A10 Thunder TPS

A10 Thunder TPS protects large networks with a 300 Gbps high-performance appliance for the most demanding requirements. The system features two dual power supplies, solid-state drives (SSDs), have no inaccessible moving parts for high availability, and has switching and routing processors to provide high-performance network processing. A10 Thunder TPS provides an own interface for management, including a console port, of message logging, email alert notifications and port mirroring. For audit records, the epoch timestamp in the header indicates when the samples were taken. It supports the common event format (CEF) open log management standard for interoperability with 3rd party SIEM and other monitoring systems. The following table describes some key characteristic for the A10 Thunder 3030S TPS.

	3030S TPS
Throughput	10 Gbps
TCP SYN Auth/sec (PPS)	3.5 million
SYN Cookie/sec (PPS)	7.5 million
Flexible Traffic Acceleration	Software

Table 1: A10 Thunder TPS characteristics

No non-TOE hardware/software/firmware is required by the TOE for operation.

1.3.1. PROTECTION LAYERS

A10 Thunder TPS scrubs traffic at multiple layers[1]:

- Hardware – A10 Thunder TPS hardware is designed to detect attacks that can be perpetrated through invalidly formed packets or using packets containing invalid option settings.
- Layer 2/3 – Traffic is compared against a set of limits and rates, including connection and connection-rate limits. DDoS Mitigation uses a default set of limits. Custom limits can be configured and applied, by configuring and applying custom GLIDs to DDoS Mitigation rules.
- Layer 4 – Traffic is scrubbed and handled based on Layer 4 type (TCP, UDP, ICMP, or other). Custom Layer 4 settings in DDoS templates can be configured, and applied to the applicable Layer 4 types within rules. For TCP or UDP, there can be applied DDoS templates for individual protocol ports within rules.

[1] OSI Model layers 1-7: Physical, Data Link, Network, Transport, Session, Presentation, Application

- Layer 7 – Traffic is scrubbed and handled based on Layer 7 application type, such as HTTP or DNS. Custom Layer 7 settings in DDoS templates can be configured, and applied to the applicable Layer 7 application types within rules. There can also be applied DDoS templates for individual application ports.

When DDoS Mitigation is enabled, traffic in excess of any of the configured rates or other checks is dropped, by default. If logging is configured, the over-limit event is also logged.

DDOS TEMPLATES

To detect and mitigate DDoS attacks in real time, the administrator can apply DDoS mitigation templates or custom countermeasures instantly.

For the Layer 4 options, the administrator can configure the following settings for individual protocol ports:

- GLID – Applies a custom set of traffic rates.
- Deny – Automatically Black Lists a source and drops its traffic.
- Permit – Automatically White Lists a source and allows its traffic.
- TCP/UDP Template – Applies protocol-specific custom settings defined in a DDoS template.

Some TCP/UDP security options can be set at the Layer 4 level within individual DDoS Mitigation rules. Other options can be configured within TCP/UDP templates, and applied to source and destination rules by binding the template to the rules.

In source rules, the administrator can use DDoS templates to apply custom mitigation settings based on application type. For example, the administrator can configure DDoS mitigation settings for HTTP traffic in a DDoS HTTP template, and apply the template to application type HTTP. The settings apply to all HTTP traffic that otherwise matches the rule. The administrator can filter based on the following application types:

- DNS over TCP.
- DNS over UDP.
- HTTP.
- Layer 4 SSL (session setup and key negotiation traffic only, not encrypted traffic).

ACOS includes DDoS Mitigation options specifically for scrubbing DNS/HTTP traffic. These options supplement the protection already provided by the system traffic limits (system defaults or defined in a custom GLID) and any Layer 4 templates. DDoS Mitigation includes features that can mitigate DDoS attacks that are based on misuse of the SSL session-setup or renegotiation requests.

1.3.2. SECURE CLIENT-SERVER TRAFFIC

The TOE can enable TCP authentication for client-to-server streams that are redirected to the A10 Thunder TPS device after the 3-way handshake has occurred. When this option is enabled, ACOS authenticates a client by replying to an ACK from the client with an ACK that contains a sequence number and other TCP values that are valid for that client-server TCP stream.

By default, ACOS drops ACKs for unknown TCP sessions. An unknown TCP session is one that is not being tracked in the ACOS session table[2]. For example, a client-to-server stream that is redirected to the A10 Thunder TPS device after the 3-way handshake has

[2] The session table is not the same as a DDoS Mitigation table. The DDoS Mitigation tables contain security entries for protected sources and destinations. The session table instead contains entries related specifically to stateful session management. For example, a TCP session is tracked in the session table, while the security status of the session's client and server (source and destination) are tracked in the source and destination DDoS Mitigation tables instead.

occurred may be legitimate traffic. However, since ACOS does not have an entry in the session table for the traffic flow, the session is unknown to ACOS.

Optionally, there can be enabled an Action-on-ACK feature. When Action-on-ACK is enabled, ACOS authenticates ACKs for unknown sessions, instead of dropping them. In this case, ACOS uses TCP authentication to validate the ACK's sender.

When Action-on-ACK is enabled, ACOS authenticates a client by replying to an ACK from the client with an ACK that contains information used for authentication. This information includes a sequence number and other TCP values that are valid for that client-server TCP stream.

- If the client replies with a valid ACK within the specified timeout, ACOS places the client on the White List. Optionally, you can configure ACOS to send a TCP Reset to the client to reset the session after authentication.
- If the client does not reply within the timeout, or sends an invalid reply, ACOS instead places the client on the Black List.

The timeout is configurable and can be 1-31 seconds.

1.3.3. DDoS Mitigation

DDoS Mitigation performs validity checks in hardware on all traffic received by the device. Traffic that passes this initial screening is further scrubbed based on traffic limits, authentication, and other checks configured in DDoS Mitigation rules:

- If the traffic passes the scrub, ACOS forwards the traffic.
- If the traffic fails the scrub, ACOS performs the configured DDoS Mitigation action (drop, by default). If logging is enabled, the event also is logged.

Based on the outcome of the rule comparison, ACOS also creates or updates entries in the applicable DDoS Mitigation tables.

Initial Scrubbing (hardware-based checks)

When DDoS Mitigation is enabled, the feature automatically performs the following checks in hardware for all inbound traffic:

- LAND Attack *
- Empty Fragment
- Micro Fragment
- IPv4 Options
- Invalid IP Fragment *
- Invalid IP Fragment Offset
- Invalid IP Header Length
- Invalid IP Flags
- Invalid IP TTL *
- No IP Payload *
- Oversized IP Payload *
- Invalid IP Payload Length *
- Invalid IP Checksum
- ICMP Ping of Death
- TCP Invalid Urgent Offset *
- TCP Short Header *
- TCP Invalid Length *
- TCP Null Flags *
- TCP Null Scan *
- TCP SYN and FIN in same packet *
- TCP XMAS Flags *
- TCP XMAS Scan *
- TCP SYN Fragment

- TCP Fragmented Header
- TCP Invalid Checksum *
- UDP Short Header *
- UDP Invalid Length *
- UDP Kerberos Frag *
- UDP Port Loopback *
- UDP Invalid Checksum *
- Runt IP Header *
- Runt TCP/UDP Header *
- IP Tunnel Mismatch *
- IP Tunnel Error *
- TCP Option Error *

(*: indicates support for both IPv4 and IPv6)

For traffic that passes all these initial checks, additional checks are performed in software, based on the default limits or configured DDoS Mitigation rules.

DDoS Mitigation Rules

DDoS Mitigation rules are used to perform software-based checks. The software-based checks are applied to traffic that passes all the hardware-based checks:

- Source-destination rule matching
  - Does the traffic match a source-destination rule? If so, the actions for that rule are performed. If not, proceed through the next checks.
- Destination rule matching
  - Does the traffic match an existing entry in the DDoS Mitigation destination IP table? If so, use the Black/White List status. Even if the destination is White Listed, enforce the traffic rates.
- Source rule matching
  - Does the traffic match an existing entry in the DDoS Mitigation source IP table? If so, use the Black/White List status. Even if the source is White Listed, enforce the traffic rates.

DDoS Mitigation Table

A10 Thunder TPS tracks the security status of traffic sources and destinations using a set of DDoS Mitigation tables. The DDoS Mitigation tables contain the DDoS Mitigation status for a given "protected object", which can be a source, destination, or source-destination pair. When applicable, the status includes the protected object's membership on the White List (permit) or Black List (deny).

The DDoS Mitigation tables are populated by a set of DDoS Mitigation rules. The DDoS Mitigation tables are used to track the security status for traffic flows. Entries can be added to the tables through dynamic learning during the authentication process. Static entries can be added manually. Each table can contain both IPv4 and IPv6 entries.

A10 Thunder TPS uses the following DDoS Mitigation tables:

- Destination IP table – Tracks security status for traffic destinations. Limits applied to destination IP addresses are intended to protect a given service or server subnet from traffic originating from any source.
- Source IP table – Tracks security status for traffic sources. Limits applied based on source IP addresses are intended to throttle excessive or malicious traffic from a given host or subnet.
- Source-Destination IP tables – Tracks security status for specific source-destination pairs. Limits that apply to specific combinations of source and destination IP addresses are useful for regulating traffic from a specific client to a

given host. These limits override the limits that apply separately to the traffic's source address and destination address.

The DDoS Mitigation tables are populated based on corresponding sets of rules, the DDoS Mitigation rules. DDoS Mitigation rules match on source or destination host or subnet address. Within source-IP rules, there can be specified the Layer 4 type, and application type. Destination rules can specify the Layer 4 type, IP protocol, and destination port. Destination rules also can contain source-destination pairs.

When DDoS Mitigation is enabled, all traffic passing through the Thunder TPS device is matched based first on destination IP address, then on source IP address. Traffic matching a specific source-destination rule is scrubbed according to that rule, rather than based on the individual destination and source rules that match.

Source-destination pairs provide custom settings for a destination based on characteristics of the source traffic. The administrator can configure a source-destination pair based on the following characteristics of source traffic:

- Layer 4 type (TCP, UDP, ICMP, or Other)
- Application type:
  - DNS over TCP
  - DNS over UDP
  - HTTP
  - Layer 4 SSL (session setup and key negotiation traffic only, not encrypted traffic)

At the Layer 4 level, the administrator can apply a GLID or a DDoS template. At the application level, the administrator can apply a DDoS template.

The option settings in a source-destination pair override any settings for those same options elsewhere in the rule. For example, to allow higher traffic rates for HTTP than for other types of traffic, the administrator can configure a custom GLID with the higher rates, and apply it to application type HTTP within a source-destination pair within the destination-IP rule.

HTTP traffic to the destination covered by the rule is allowed to use the higher rates in the custom GLID. However, non-HTTP traffic to the rule's destination is rate limited based either on the default rates, or on custom rates applied elsewhere within the rule.

BLACK/WHITE LISTING

Traffic sources and destinations are tracked in DDoS Mitigation tables. Within the DDoS Mitigation tables, sources or destinations can be flagged with Black List status or White List status:

- White List – Sources and destinations with White List status are trusted. Traffic received from trusted sources is still rate limited.
- Black List – Traffic from sources or to destinations with Black List status is dropped.

New traffic to Thunder TPS devices is subject to authentication before the traffic is passed on. Authenticated traffic is placed on a White List, and future traffic from that source is allowed through, subject to rate limiting. Traffic that fails authentication is placed on a Black List instead. Future traffic from that source is dropped until the Black List entry ages out.

Role of the White List: Authenticated traffic is added to a White List, and future traffic from that source is passed on without needing re-authentication.

Role of the Black List: For traffic that fails authentication, the configured action is taken (drop, by default) and the client is placed on the Black List. Subsequent traffic from that source is dropped, regardless of destination, until the Black List entry ages out.

Dynamic Black/White Listing applies only to source IPs. The DDoS Mitigation tables are used to track the security status for traffic flows. Entries can be added to the tables through dynamic learning during the authentication process. For example, when a BGP neighbor is added, ACOS automatically creates a dynamic source-IP entry. For an IPv4 BGP neighbor, an entry in the source IPv4 DDoS Mitigation table is created. Since the entry is dynamic, it ages out if unused, and consequently is removed from the table. However, a new entry is added the next time traffic from the neighbor is received. The age time of the default source IP rule is used.

Permanent White Listing can be configured for source IPs, and Permanent Black Listing can be configured for both source and destination IPs.

DDoS Mitigation Threshold

DDoS Mitigation thresholds are calculated based on regular intervals. At the beginning of each interval, the counter for each threshold is set to 0. If traffic exceeds a threshold within the same interval, the over-limit traffic is dropped. (Or, if the administrator configures a different action, that action is performed.) The counter for each interval is then reset to 0 at the beginning of the next rate interval.

By default, each interval is one-tenth of a second long (0.1 seconds). This tenth-of-a-second granularity allows DDoS Mitigation to enforce rate limits even on very brief traffic bursts. This is the default DDoS Mitigation rate interval.

Optionally, the administrator can set the rate interval to one full second instead. The one second rate interval is helpful for testing the feature, since much less traffic is required to exceed the same configured thresholds. Using the one-second rate interval, DDoS Mitigation rate limits can be exceeded by only a tenth of the traffic required to exceed the same limits using the tenth-of-a-second rate interval.

1.3.4. Application-Layer Security

ACOS includes DDoS Mitigation options specifically for scrubbing traffic for TCP/UDP anomalies and for attacks that exploit the TCP/UDP protocol. These options supplement the protection already provided in hardware and by the system traffic limits (system defaults or defined in a custom GLID).

ACOS includes DDoS Mitigation options specifically for scrubbing DNS traffic. These options supplement the protection already provided by the system traffic limits (system defaults or defined in a custom GLID) and any Layer 4 templates

ACOS includes DDoS Mitigation options specifically for scrubbing DNS/HTTP traffic. These options supplement the protection already provided by the system traffic limits (system defaults or defined in a custom GLID) and any Layer 4 templates.

ACOS includes DDoS Mitigation options specifically for scrubbing SSL traffic at Layer 4. These options supplement the protection already provided by the system traffic limits (system defaults or defined in a custom GLID) and any other templates.

1.3.5. CLI COMMANDS FOR CONFIGURING AND MANAGING DDOS MITIGATION FEATURES

A10 Thunder TPS employs CLI commands for configuring and managing DDoS Mitigation features. The CLI is organized in two main management levels, described in the following:

- User EXEC – Basic operational commands, including ping and some show commands.
- Privileged EXEC – More extensive set of operational commands, including file management commands, clear commands, and all show commands. The following describes the configuration level commands, available only for the Privileged EXEC level:
    - Global configuration – Configuration commands that apply on a system wide basis. With a few exceptions, these commands appear in the running-configuration after they are issued, and are written to the startup-configuration when the configuration is saved (write memory command). Most DDoS Mitigation configuration commands are at this level.
    - Routing configuration – Configuration commands that apply to a specific routing protocol, such as Border Gateway Protocol (BGP).
    - Interface configuration – Configuration commands that apply only to a specific interface.
    - GLID (rate limit) commands – Configuration commands that apply to a specific GLID.
    - DDoS – Configuration commands for DDoS Mitigation features.

The clear commands are available at any configuration level, and at the main management level Privileged EXEC. The show commands are available at all levels.

To access the User EXEC level commands, an administrator has to perform a login with a username and a password. To access the Privileged EXEC level commands, an administrator has to perform another login with another password.

1.3.6. GUI AND AXAPI FOR CONFIGURING AND MANAGING DDOS MITIGATION FEATURES

A10 Thunder TPS also employs a GUI and the aXAPI open RESTful API for configuring and managing DDoS Mitigation features. The GUI and aXAPI support a single management level, described in the following:

- Privileged EXEC – As with this level when accessing via the CLI, supports the full set of management operations available.

GUI and aXAPI access for the Privileged EXEC level involves logging in (GUI) or authenticating (aXAPI) with a username and a password.

1.3.7. A10 THUNDER TPS FEATURES

The following describes A10 Thunder TPS features to detect and mitigate multi-vector DDoS attacks with unprecedented performance scalability and deployment flexibility.

MULTI-LEVEL DDOS PROTECTION FOR SERVICE AVAILABILITY

A10 Thunder TPS is able to detect and mitigate a broad level of attacks, even if multiple attacks hit the network simultaneously:

- **Complete multi-vector attack protection:** Service availability is realized by detecting and mitigating DDoS attacks of many types, whether they are pure volumetric, protocol or resource attacks, or even application-level attacks:
    - Volumetric attacks, such as SYN Floods and DNS amplification attacks are designed to flood and saturate a victim's network connection, thus

rendering services unavailable. Thunder TPS implements multi-protocol rate limiting to prevent sudden surges of illegitimate traffic from overwhelming network and server resources.
    - Protocol attacks, such as ping of death and IP anomalies, are aimed at exhausting a victim's protocol stack so it cannot respond to legitimate traffic. Thunder TPS detects and mitigates up to 60 anomaly attacks in hardware to stop them before system CPUs have to be involved.
    - Resource attacks, such as fragmentation attacks or HTTP Slowloris, are aimed at exhausting a victim's network or application resources. A resource attack renders a victim's services unusable, with minimal bandwidth usage. Thunder TPS recognizes many resource attacks and can deny malicious client access.
    - Application attacks such as HTTP GET floods are specifically exploiting a weakness in an application's function or trying to make it unavailable. With A10's aFleX feature, Thunder TPS is able to perform deep packet inspection (DPI) on incoming packets and take defined actions to protect the application.
- **Hitless redirect (action on ACK):** When deployed in asymmetric mode, Thunder TPS can perform TCP authentication on established sessions. This means that for legitimate clients, the session will not be broken.

PERFORMANCE AND SCALE TO ADDRESS THE LARGEST ATTACKS

Over the last few years, DDoS attacks have rapidly proliferated in terms of bandwidth (Gbps) and packets per second (PPS). Thunder TPS is equipped with high-performance FPGA hardware and powerful Intel Xeon CPUs to mitigate any scale of attack:

- **Performance to address the largest attacks:** Mitigation capacity to 300 Gbps (or 2.4 Tbps in a cluster) of throughput ensures the largest DDoS attacks to be handled effectively. FTA enabled Thunder TPS models can be equipped with high-performance FPGA-based FTA technology to detect and mitigate up to 60 common attack vectors rapidly, before the Intel CPUs are involved. More complex application-layer (L7) attacks (HTTP, SSL, DNS, etc.) are processed by Intel Xeon CPUs, so that high-performance system scaling is maintained even for multi-vector attacks. For models without FPGA-based FTA technology, including Thunder 3030S TPS, these same attack vectors are detected in software by the CPU complex.
- **Large threat intelligence class lists:** 63 individual lists, each containing up to 16 million list entries, can be defined to support up to 96 million class list entries. This allows a user to utilize data from IP reputation databases, in addition to the dynamically generated entries of black/white lists.
- **Simultaneous protected objects:** To protect entire networks with many connected users and services, the A10 Thunder TPS is able to simultaneously monitor a great number of hosts or subnets.

FLEXIBLE DEPLOYMENT FOR EASE OF INTEGRATION:

For network operators, it is critical that a DDoS Mitigation solution can easily be inserted into the existing network architecture, so that the network remains prepared for imminent DDoS threats:

- **Easy network integration:** With multiple performance options and flexible deployment models for inline and out-of-band operations, including both routed and transparent operation modes, A10 Thunder TPS can be integrated into any network architecture, of any size. And, with aXAPI, the open RESTful API, A10 Thunder TPS can easily be integrated into third-party detection solutions.

1.3.7.1. aXAPI OPEN RESTFUL API

With the aXAPI open RESTful API, A10 Thunder TPS enables integration to a vendor custom or third-party detection solutions.

The A10 Thunder TPS aXAPI is a REST-based API enabling remote interaction from third-party applications to control the server load balancer. The comprehensive set of instructions available allows management functions to be quickly integrated for maximum flexibility.

The aXAPI REST (Representational State Transfer) style XML API is being designed to use HTTPS with a request/response model to exchange data over HTTPS by default, and allows commands to be issued by a simple, single-line HTTP command instead of a complicated XML definition with many different object definitions.

The following figure 5 describes the communication between aXAPI and a third-party application.

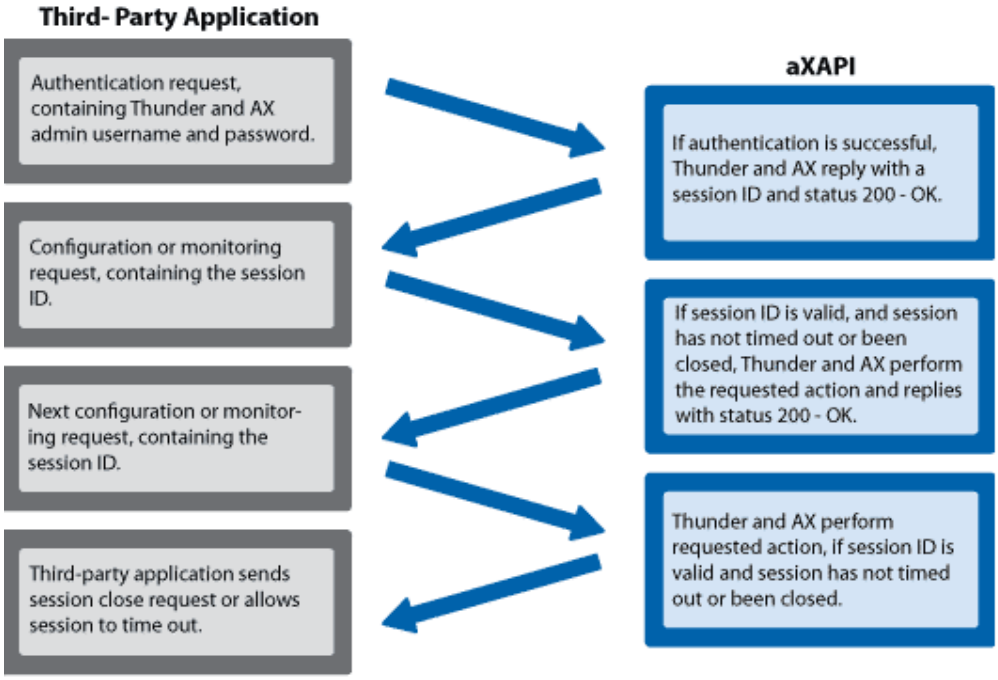

Figure 5: aXAPI Communication

1.3.8. ACOS TECHNOLOGY PLATFORM

A10 Thunder TPS devices use the embedded Advanced Core Operating System (ACOS) architecture, which is built on top of the Symmetric Scalable Multi-Core Processing (SSMP). The ACOS platform leverages the Shared Memory Architecture and Flexible Traffic Accelerator (FTA) to efficiently utilize multi-core processors and scale performance linearly with increasing CPU/processor density.

FTA is a high-performance intelligent network I/O technology that can balance application traffic flows equitably across processor cores. ACOS maximizes the utility of all processor cores by distributing traffic equally and making the shared memory available to all cores.

The FTA logic can be implemented either as software running within a standard x86 processor or a Field Programmable Gate Array (FPGA) semiconductor. Thunder 3030S TPS implements it in software. The FTA performs certain hardware-based security checks for each packet and can discard suspicious traffic before it can impact system performance.

The combined effect of the Shared Memory Architecture and FTA provides customers to scale their application and security services with the speed of their network backbone. See figure 6 for an architecture overview of ACOS.

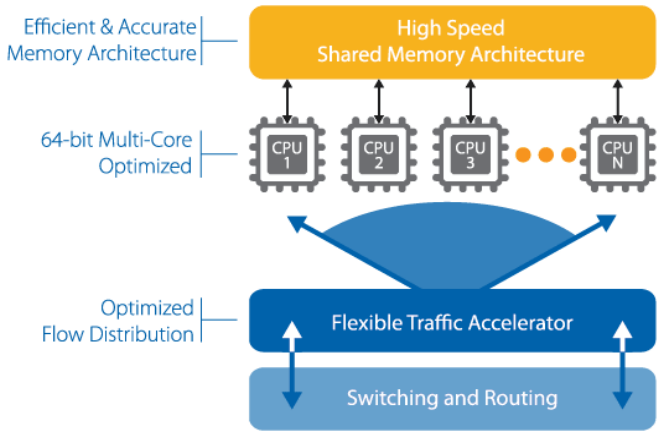

Figure 6: ACOS Advanced Core Architecture

The inherently flexible, software-based nature of ACOS has evolved and expanded the feature set into the Threat Protection System (TPS) product line that detect and mitigate DDoS attacks.

SWITCHING AND ROUTING

Switching and routing processors provide high-performance network processing.

INTEL XEON CPU

Application-layer attacks regarding among others HTTP, SSL and DNS, are processed by Intel Xeon CPUs.

HIGH SPEED SHARED MEMORY ARCHITECTURE

The Shared Memory Architecture shall allow all processors to share common memory and system state simultaneously, which improves the performance of the multi-core processor architecture.

1.4. NOTATIONS AND FORMATTING

The notations and formatting used in this ST are consistent with version 3.1 Revision 5 of the Common Criteria (CC).

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Deleted words are denoted by ~~strike-through text~~.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized* text in square brackets, [*Selection value*].

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value with bold face in square brackets, [**Assignment_value**].

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number).

Assets: Assets to be protected by the TOE are given names beginning with "AS." – e.g. AS.CLASSIFIED_INFO.

Assumptions: TOE security environment assumptions are given names beginning with "A."- e.g., A.Security_Procedures.

Threats: Threat agents are given names beginning with "TA." – e.g., TA.User. Threats to the TOE are given names beginning with "TT." – e.g., TT.Filter_Fails. TOE security environment threats are given names beginning with "TE."-- e.g., TE.Crypto_Fails.

Policies: TOE security environment policies are given names beginning with "P."—e.g., P.Information_AC.

Objectives: Security objectives for the TOE and the TOE environment are given names beginning with "O." and "OE.", respectively, - e.g., O.Filter-msg and OE.Clearance.

2. CC CONFORMANCE CLAIM (ASE_CCL)

This TOE and ST are conformant with the following specifications:

- CC Part 2: Security functional components, April 2017, Version 3.1, Revision 5, conformant.
- CC Part 3: Security assurance components, April 2017, Version 3.1, Revision 5, conformant, EAL2 augmented with ALC_FLR.1.
- Assurance level: EAL2 augmented with ALC_FLR.1.
- Protection Profile: none.
- Extended SFRs: none.

3. SECURITY PROBLEM DEFINITION (ASE_SPD)

3.1. THREATS TO SECURITY

3.1.1. ASSETS

Assets	Description
AS.HW_CHECKS	DDoS Mitigation hardware-based checks for all inbound traffic.
AS.SW_CHECKS	DDoS Mitigation software-based checks, by use of DDoS Mitigation rules, for all traffic that passes the hardware-based checks.
AS.TARGET	Target system services, resources and information.

3.1.2. THREAT AGENTS

Threat Agents	Description
TA.ATTACKER	A person/company with skills and resources to prevent the TOE in any way necessary to mitigate DDoS attacks, like: • Volumetric attacks: brute-force assaults (e.g. launched using botnets), which attempt to consume as many network resources as possible on the target system. • Protocol attacks: directing of a high rate of invalid traffic (invalidly formed packets or packets with protocol abnormalities) toward the target system, to overwhelm the system's resources. • Resource attacks: abusing of legitimately formed traffic in an attempt to overwhelm resources on the target system. • Application-layer attacks: TCP, UDP, DNS, HTTP, and SSL. The person/company can use a volumetric attack to provide a diversion for more malicious and targeted network intrusion (e.g. identity theft).
TA.ADMIN	Authorized person/process that performs configuration/setup of the TOE to ensure that the TOE operates according to the needs of the target network system.

3.1.3. IDENTIFICATION OF THREATS

3.1.3.1. THREATS TO THE TOE

Threats to the TOE	**Description**
TT.TAMPERING	The TOE may be subject to physical attack that may compromise information and data processing.
Threat agent:	TA.ATTACKER
Assets:	AS.HW_CHECKS and AS.SW_CHECKS
Attack method:	A person/company tampers with the TOE to: • Change or remove DDoS Mitigation validity checks. • Change or remove DDoS Mitigation rules.
TT.MALFUNCTION	The TOE may malfunction which may compromise information and data processing.
Threat agent:	TA.ATTACKER
Assets:	AS.HW_CHECKS, AS.SW_CHECKS and AS.TARGET

Threats to the TOE	Description
Attack method:	A malfunction in the TOE implies errors with: • DDoS Mitigation validity checks. • DDoS Mitigation rules. A malfunction in the TOE implies unauthorized access to services and resources at the target system.
TT.BYPASSING	Bypassing of a security mechanism may compromise information and data processing in the TOE.
Threat agent:	TA.ATTACKER
Assets:	AS.HW_CHECKS, AS.SW_CHECKS and AS.TARGET
Attack method:	A person/company bypass a security mechanism in the TOE to: • Change or remove DDoS Mitigation validity checks. • Change or remove DDoS Mitigation rules. • Obtain unauthorized access to services and resources at the target system.
TT.MISCONFIG	Misconfiguration of TOE, making the TOE inoperable.
Threat agent:	TA.ADMIN
Assets:	AS.HW_CHECKS, AS.SW_CHECKS and AS.TARGET
Attack method:	During service or production the administrator unintentionally performs incorrect configuration/setup of the TOE, leading to following: • Making the TOE inoperable. • Updates concerning security in the TOE are missed. • Unauthorized access to services and resources at the target system.

3.1.3.2. THREATS TO THE TOE ENVIRONMENT

Not applicable.

3.2. ORGANIZATIONAL SECURITY POLICIES

Organizational security Policies	Description
P.PATCH	The patch policy for the TOE environment must be sufficient for stopping all known, publicly available vulnerabilities in the TOE environment software.
P.AUDIT	To trace responsibilities on all security-related activities, security-related events shall be recorded and maintained and reviewed.
P.SECURE_MANAGEMENT	The TOE shall provide management means for the authorised administrator to manage the TOE in a secure manner.

3.3. ASSUMPTIONS

Assumptions	Description
A.PHYSICAL_SECURITY	The TOE shall be located in physically secure environment that can be accessed only by the authorized administrator.

Assumptions	Description
A.SECURITY_MAINTENANCE	When the internal network environment changes due to change in the network configuration, host increase/ decrease and service increase/ decrease, etc., the changed environment and security policy shall immediately be reflected in the TOE operation policy so that security level can be maintained to be the same as before.
A.TRUSTED_ADMIN	The authorized administrator of the TOE shall not have any malicious intention, receive proper training on the TOE management, and follow the administrator guidelines.

4. SECURITY OBJECTIVES (ASE_OBJ)

4.1. TOE SECURITY OBJECTIVES

Security Objectives	Description
O.ID_AUTH	The administrator roles must identify and authenticate to the TOE prior to getting access to the functions and data.
O.ACCESS	The TOE must allow only authorized administrators to access the system.
O.AUDIT	The TOE shall record and maintain security-related events in order to enable tracing of responsibilities for security-related acts and shall provide means to review the recorded data
O.DATA_PROTECTION	The TOE shall protect TSF data stored in the TOE from unauthorized exposure, modification and deletion.
O.INTEGRITY	The TOE must ensure the integrity of all system data.
O.MANAGEMENT	The TOE shall provide means for the authorized administrator of the TOE to efficiently manage the TOE in a secure manner.
O.SELF_TEST	DDoS Mitigation configurable rate interval shall be tested.

4.2. OPERATIONAL ENVIRONMENT SECURITY OBJECTIVES

Security Objectives	Description
OE.TRUSTED_ADMIN	The authorized administrator of the TOE shall not have any malicious intention, receive proper training on the TOE management, and follow the administrator guidelines.
OE.PHYSICAL_SECURITY	The TOE shall be located in physically secure environment that can be accessed only by the authorized administrator.
OE.SECURITY_MAINTENANCE	When the internal network environment changes due to change in the network configuration, host increase/ decrease and service increase/ decrease, etc., the changed environment and security policy shall immediately be reflected in the TOE operation policy so that security level can be maintained to be the same as before.
OE.TIME_STAMP	The TOE shall accurately record the security related events by using the reliable time stamps provided by the TOE operational environment.

4.3. SECURITY OBJECTIVES RATIONALE

Threats/ Policies/ Assumptions / Objectives	TT.TAMPERING	TT.MALFUNCTION	TT.BYPASSING	TT.MISCONFIG	P.PATCH	P.AUDIT	P.SECURE_MANAGEMENT	A.PHYSICAL_SECURITY	A.SECURITY_MAINTENANCE	A.TRUSTED_ADMIN
TOE Security Objectives										
O.ID_AUTH		X	X							
O.ACCESS		X	X							
O.AUDIT	X	X		X		X				
O.DATA_PROTECTION	X	X	X							
O.INTEGRITY		X	X							
O.MANAGEMENT					X	X	X			
O.SELF_TEST		X								
Operational Environment Security Objectives										
OE.TRUSTED_ADMIN				X	X	X	X			X
OE.PHYSICAL_SECURITY	X							X		
OE.SECURITY_MAINTENANCE									X	
OE.TIME_STAMP						X				

Table 2: Mapping of Objectives to Threats, Policies and Assumptions.

TT.TAMPERING:
A physical attack towards the TOE can compromise its information and data processing. The TOE, placed in a physically secure area (OE.PHYSICAL_SECURITY), must protect the TSF data (O.DATA_PROTECTION) and record security events (O.AUDIT).

TT.MALFUNCTION:
A TOE malfunction can compromise information and data processing in the TOE.
The TOE shall test rate intervals (O.SELF_TEST), protect the TSF data (O.DATA_PROTECTION), record security events (O.AUDIT) and ensure the integrity of all system data (O.INTEGRITY). Administrators must identify and authenticate to the TOE, which allows only authorized administrators access (O.ID_AUTH, O.ACCESS).

TT.BYPASSING:
Bypassing of a security mechanism can compromise information and data processing in the TOE.
The TOE shall protect the TSF data (O.DATA_PROTECTION) and ensure the integrity of all system data (O.INTEGRITY). Administrators must identify and authenticate to the TOE, which allows only authorized administrators access (O.ID_AUTH, O.ACCESS).

TT.MISCONFIG:
Misconfiguration of TOE can make the TOE inoperable.
The TOE shall record security events (O.AUDIT). The authorized administrator is non-hostile and is trained to appropriately manage and administer the TOE (OE.TRUSTED_ADMIN).

P.PATCH:

The patch policy for the TOE environment should be sufficient for stopping all known, publicly available vulnerability in the TOE environment software.
The authorized administrator of the TOE shall manage the TOE in a secure manner and follow the administrator guidelines (O.MANAGEMENT, OE.TRUSTED_ADMIN).

P.AUDIT:
To trace responsibilities on all security-related activities, security-related events should be recorded and maintained and reviewed.
The TOE shall record timestamped security events (O.AUDIT, OE.TIME_STAMP), available for the authorized administrator of the TOE who shall manage the TOE in a secure manner and follow the administrator guidelines (O.MANAGEMENT, OE.TRUSTED_ADMIN).

P.SECURE_MANAGEMENT:
The TOE should provide management means for the authorised administrator to manage the TOE in a secure manner.
The authorized administrator of the TOE shall manage the TOE in a secure manner and follow the administrator guidelines (O.MANAGEMENT, OE.TRUSTED_ADMIN).

A.PHYSICAL_SECURITY:
The TOE shall be located in physically secure environment only accessed by the authorized administrator (OE.PHYSICAL_SECURITY).

A.SECURITY_MAINTENANCE:
Changed environment and security policy shall be reflected in the TOE operation policy (OE.SECURITY_MAINTENANCE).

A.TRUSTED_ADMIN:
The authorized administrator of the TOE shall not have any malicious intention, receive proper training on the TOE management, and follow the administrator guidelines (OE.TRUSTED_ADMIN).

5. EXTENDED COMPONENTS DEFINITION (ASE_ECD)

Not applicable.

6. SECURITY REQUIREMENTS (ASE_REQ)

6.1. SECURITY FUNCTIONAL REQUIREMENTS (SFRS)

Functional Class	Functional Class Description	Functional Components
FAU	Security audit	FAU_GEN.1, FAU_SAR.1
FDP	User data protection	FDP_ACC.1, FDP_ACF.1, FDP_IFC.2, FDP_IFF.1
FIA	Identification and authentication	FIA_ATD.1, FIA_UAU.1, FIA_UID.2
FMT	Security management	FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1
FPT	Protection of the TSF	FPT_STM.1, FPT_TST.1

Table 3: Security Functional Requirements

6.1.1. SECURITY AUDIT (FAU)

6.1.1.1. FAU_GEN.1 AUDIT DATA GENERATION

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the [*not specified*] level of audit; and
c) [**Violating of DDoS Mitigation checks**].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**None**].

6.1.1.2. FAU_SAR.1 AUDIT REVIEW

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [**the Privileged EXEC administrator**] with the capability to read [**all information**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.2. User Data Protection (FDP)

6.1.2.1. FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [**Administrator Access Control SFP**] on [subjects: **Privileged EXEC administrator**, objects: **commands**, operations: **execute**].

6.1.2.2. FDP_ACF.1 Security attribute based access control

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [**Administrator Access Control SFP**] to objects based on the following: [subjects: **Privileged EXEC administrator**; subject attributes: **admin ID, password**; object: **file management, clear and configuration commands**; object attributes: **none**].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**no additional rules**].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**no additional rules**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**no additional rules**].

6.1.2.3. FDP_IFC.2 Complete information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.2.1 The TSF shall enforce the [**DDoS Mitigation information flow control SFP**] on [subjects: **clients**, information: **all traffic received by the TOE**] and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

6.1.2.4. FDP_IFF.1 Simple security attributes

Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the **[DDoS Mitigation information flow control SFP]** based on the following types of subject and information security attributes: [subjects: **clients**, subject attributes: **source IP, destination IP, destination port**, information: **all traffic received by the TOE**, information attributes: **amount of traffic rate limits including: packets per interval, concurrent connections, new connection requests per interval; and also over-limit action**].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [

- **The DDoS Mitigation rules/tables contain security entries for protected sources and destinations for the client;**

- **Entries added to the DDoS Mitigation rules/tables through dynamic learning during the authentication process;**
- **Traffic from sources not dropped due to traffic limits**].

FDP_IFF.1.3 The TSF shall enforce the [**DDoS Mitigation automatically initial scrubbing (hardware-based checks) for all inbound traffic**].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [**no additional information flow control SFP rules**].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [**no additional information flow control SFP rules**].

6.1.3. IDENTIFICATION AND AUTHENTICATION (FIA)

6.1.3.1. FIA_ATD.1 USER ATTRIBUTE DEFINITION

Dependences: None.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**administrator ID, password**].

6.1.3.2. FIA_UAU.1 TIMING OF AUTHENTICATION

Dependences: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow **[administrator identification]** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.3. FIA_UID.2 USER IDENTIFICATION BEFORE ANY ACTION

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.4. SECURITY MANAGEMENT (FMT)

6.1.4.1. FMT_MOF.1 MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOUR

Dependences: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MOF.1.1 The TSF shall restrict the ability to [*determine the behaviour of, disable, enable, modify the behaviour of*] the functions **[for configuration and managing DDoS Mitigation features]** to **[Privileged EXEC administrator]**.

6.1.4.2. FMT_MSA.1 MANAGEMENT OF SECURITY ATTRIBUTES

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [**administrator Access Control SFP**] to restrict the ability to [*change_default, query, modify, delete*] the security attributes [**DDOS Mitigation table information**] to [**Privileged EXEC administrator**].

6.1.4.3. FMT_MSA.3 STATIC ATTRIBUTE INITIALISATION

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [**administrator Access Control SFP**] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**Privileged EXEC administrator**] to specify alternative initial values to override the default values when an object or information is created.

6.1.4.4. FMT_SMF.1 SPECIFICATION OF MANAGEMENT FUNCTIONS

Dependencies: None.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [**message logging, email alert notification, port mirroring**].

6.1.4.5. FMT_SMR.1 SECURITY ROLES

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles **[User EXEC administrator, Privileged EXEC administrator]**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.5. PROTECTION OF THE TSF (FPT)

6.1.5.1. FPT_STM.1 RELIABLE TIME STAMPS

Dependencies: None.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.1.5.2. FPT_TST.1 TSF TESTING

Dependencies: None.

FPT_TST.1.1 The TSF shall run a suite of self tests [*at the request of the authorised user*] to demonstrate the correct operation of [***DDoS Mitigation configurable rate interval***].

FPT_TST.1.2 The TSF shall provide authorised users with the capability to verify the integrity of [***No TSF data***].

FPT_TST.1.3 The TSF shall provide authorised users with the capability to verify the integrity of [***No parts of TSF***].

6.2. SECURITY ASSURANCE REQUIREMENTS (SARS)

The assurance level of the TOE is EAL2 augmented with ALC_FLR.1.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.1 Basic flaw remediation
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Table 4: Assurance requirements

6.3. SECURITY REQUIREMENTS RATIONALE

6.3.1. RELATION BETWEEN SFRS AND SECURITY OBJECTIVES

Requirements / Objectives	FAU_GEN.1	FAU_SAR.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.2	FDP_IFF.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.2	FMT_MOF.1	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1	FPT_STM.1	FPT_TST.1
O.ID_AUTH							X	X	X							
O.ACCESS			X	X	X	X		X	X		X	X				
O.AUDIT	X	X													X	
O.DATA_PROTECTION	X		X	X				X	X	X	X		X			
O.INTEGRITY			X	X						X	X	X				
O.MANAGEMENT		X								X	X	X	X	X		
O.SELF_TEST																X

Table 5: Tracing of functional requirements to objectives

6.3.1.1. O.ID_AUTH

The administrator should identify and authenticate to the TOE prior to getting access to the functions and data.
FIA_UID.2 requires administrators to be identified before they are able to perform any other actions. **FIA_UAU.1** requires administrators to be authenticated before they are

able to perform any other actions, except identification. **FIA_ATD.1** defines security attributes of subjects used to enforce the authentication policy of the TOE.

6.3.1.2. O.ACCESS

The TOE should allow only authorized administrators to access the system.
FMT_MSA.3 defines static attribute initialization for the Administrator Access Control SFP. **FMT_MSA.1** specifies which administrator roles can access security attributes. **FDP_ACC.1** requires the TOE to enforce Access Control SFP. **FDP_ACF.1** specifies the attributes used to enforce Access Control SFP. **FDP_IFC.2** requires the TOE to enforce Information Flow Control SFP. **FDP_IFF.1** specifies the attributes used to enforce Information Flow Control SFP. **FIA_UID.2** requires administrators to be identified before they are able to perform any other actions. **FIA_UAU.1** requires administrators to be authenticated before they are able to perform any other actions, except identification.

6.3.1.3. O.AUDIT

The TOE should record and maintain security-related events in order to enable tracing of responsibilities for security-related acts and shall provide means to review the recorded data.
FAU_GEN.1 and **FPT_STM.1** requires the TOE to record security events with timestamp; and **FAU_SAR.1** provides administrators the capability to read the audit records.

6.3.1.4. O.DATA_PROTECTION

The TOE should protect TSF data stored in the TOE from unauthorized exposure, modification and deletion.
FAU_GEN.1 requires the TOE to record security events. **FDP_ACC.1** requires the TOE to enforce Access Control SFP. **FDP_ACF.1** enforces Access Control SFP by file management, clear and configuration commands. **FIA_UID.2** and **FIA_UAU.1** require administrators to be identified and authenticated before they are able to perform any other actions on the TOE. **FMT_MOF.1** requires the TOE to provide the ability to manage functions of the TOE only to the Privileged EXEC administrator of the TOE. **FMT_MSA.1** specifies which administrator roles can access security attributes. **FMT_SMF.1** supports this objective by identifying the corresponding management functions.

6.3.1.5. O.INTEGRITY

The TOE should ensure the integrity of all system data.
FDP_ACC.1 and **FDP_ACF.1** ensure that the TOE enforces Access Control SFP with the necessary attributes. **FMT_MOF.1** requires the TOE to provide the ability to configure managing functions of the TOE only to the Privileged EXEC administrator of the TOE. **FMT_MSA.1 and FMT_MSA.3** ensure that only the Privileged EXEC administrator can respectively access security attributes and override default values.

6.3.1.6. O.MANAGEMENT

The TOE should provide means for the authorized administrator of the TOE to efficiently manage the TOE in a secure manner.
FMT_MSA.3 defines static attribute initialization for the Administrator Access Control SFP. **FMT_MOF.1** requires the TOE to provide the ability to manage functions of the TOE only to the Privileged EXEC administrator of the TOE. **FMT_SMF.1** supports this objective by identifying the corresponding management functions. **FMT_SMR.1** requires the TOE to maintain separate administrator roles. **FAU_SAR.1** provides the Privileged EXEC administrators the capability to read all information from the audit records. **FMT_MSA.1** specifies which administrator roles can access security attributes.

6.3.1.7. O.SELF_TEST

DDoS Mitigation configurable rate interval should be tested.
FPT_TST.1 requires the TOE to run tests of DDoS Mitigation thresholds at the request of the administrator to demonstrate the correct operation of DDoS Mitigation configurable rate intervals.

6.3.2. SFR DEPENDENCIES

The table below shows the dependencies of the security functional requirement of the TOE and gives a rationale for each of them if they are included or not.

Security Functional Requirement	Dependency	Dependency Rationale
FAU_GEN.1 Audit data generation	FPT_STM.1 Reliable time stamps	Included
FAU_SAR.1 Audit review	FAU_GEN.1 Audit data generation	Included
FDP_ACC.1 Subset access control	FDP_ACF.1 Security attribute based access control	Included
FDP_ACF.1 Security attribute based access control	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	Included
FDP_IFC.2 Complete information flow control	FDP_IFF.1 Simple security attributes	Included
FDP_IFF.1 Simple security attributes	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	Included[3]
FIA_ATD.1 User attribute definition	None	
FIA_UAU.1 Timing of authentication	FIA_UID.1 Timing of identification	Included[4]
FIA_UID.2 User identification before any action	None	
FMT_MOF.1 Management of security functions behaviour	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles	Included
FMT_MSA.1 Management of security attributes	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	Included
FMT_MSA.3 Static attribute initialisation	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Included
FMT_SMF.1 Specification of Management Functions	None	
FMT_SMR.1 Security roles	FIA_UID.1 Timing of identification	Included[5]

[3] FDP_IFF.1 has a dependency to FDP_IFC.1 which is covered by FDP_IFC.2.
[4] FIA_UAU.1 has a dependency to FIA_UID.1 which is covered by FIA_UID.2.

Security Functional Requirement	Dependency	Dependency Rationale
FPT_STM.1 Reliable time stamps	None	
FPT_TST.1 TSF testing	None	

Table 6: SFR's dependencies and rationale

6.3.3. SAR RATIONALE

The SARs specified in this ST are according to EAL2 augmented with ALC_FLR.1.

[5] FMT_SMR.1 has a dependency to FIA_UID.1 which is covered by FIA_UID.2.

7. TOE SUMMARY SPECIFICATION (ASE_TSS)

7.1. TOE SECURITY FUNCTIONS SPECIFICATION

This section describes the security functions provided by the TOE to meet the security functional requirements specified for the TOE in section 6.1 Security Functional Requirements (SFRs).

The table below shows the mapping between the SFRs and the implementing security functions, and a description is given in the following subsections.

Requirements / Functions	FAU_GEN.1	FAU_SAR.1	FDP_ACC.1	FDP_ACF.1	FDP_IFC.2	FDP_IFF.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.2	FMT_MOF.1	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1	FPT_STM.1	FPT_TST.1
SF.AUTHENTICATION							X	X	X							
SF.ACCESS			X	X	X	X		X	X		X	X				
SF.AUDIT	X	X													X	
SF.PROTECTION	X		X	X				X	X	X	X		X			
SF.INTEGRITY			X	X						X	X	X				
SF.MANAGEMENT		X								X	X	X	X	X		
SF.TEST																X

Table 7: Mapping SFRs to security functions

7.1.1. SF.AUTHENTICATION

The administrators identify themselves to the TOE and are authenticated prior to getting access to their functions and data.

A10 Thunder TPS provides advanced features for (securing) management access to the device. On a PC connected to a network that can access to a dedicated management interface, the administrator can open an SSH connection to the IP address of the management interface.

User EXEC level:
At the login prompt, the administrator enters the username "admin", and at the password prompt, the administrator enters the admin password, (default password is "a10"). If the admin username and password are valid, the command prompt for the User EXEC level of the CLI appears. The User EXEC level allows the administrator to enter a few basic commands, including ping and some show commands.

Privileged EXEC level:
To access the Privileged EXEC level of the CLI and allow access to all configuration levels, the administrator enters the "enable" command. At the password prompt, the administrator enters the enable password. This password is not the same as the admin password, although it is possible to configure the same value for both passwords. If the enable password is correct, the command prompt for the Privileged EXEC level of the CLI appears. To access the requested configuration level, the administrator has to enter the relevant configuration level command. Then a command prompt including configuration level information appears.

A10 Thunder TPS also employs a GUI and the aXAPI open RESTful API for configuring and managing DDoS Mitigation features. The GUI and aXAPI support a single management level, described in the following:

- Privileged EXEC – As with this level when accessing via the CLI, supports the full set of management operations available.

GUI and aXAPI access for the Privileged EXEC level involves logging in (GUI) or authenticating (aXAPI) with a username and a password.

7.1.2. SF.ACCESS

The TOE allows only authorized administrators to access the system.

A10 Thunder TPS employs CLI commands for configuring and managing DDoS Mitigation features, where the CLI is organized in two main management levels User EXEC and Privileged EXEC. To access the User EXEC level of the CLI, the administrator must enter the username "admin" at the login prompt, before the admin password for this level is used. To access the Privileged EXEC level of the CLI (and allow access to all configuration levels), the administrator enters the "enable" command, before the admin password for this level is used.

The User EXEC level makes use of basic operational commands, including ping and some show commands. The Management level Privileged EXEC employs an extensive set of operational commands, including file management commands, clear commands, and all show commands. In addition, the configuration level commands are available only for the Privileged EXEC level, including, Global configuration, Routing configuration, Interface configuration, GLID (rate limit) and DDoS. To access the Privileged EXEC level commands, an administrator has to perform a login with a username and a password.

DDoS Mitigation performs validity checks in hardware on all traffic received by the device. Traffic that passes this initial screening is further scrubbed based on traffic limits, authentication, and other checks configured in DDoS Mitigation rules.

Traffic sources and destinations are tracked in DDoS Mitigation tables, which are managed by the Privileged EXEC administrator. Within the DDoS Mitigation tables, sources or destinations can be flagged with Black List status or White List status.

A10 Thunder TPS also employs a GUI and the aXAPI open RESTful API for configuring and managing DDoS Mitigation features. The GUI and aXAPI support a single management level, described in the following:

- Privileged EXEC – As with this level when accessing via the CLI, supports the full set of management operations available.

GUI and aXAPI access for the Privileged EXEC level involves logging in (GUI) or authenticating (aXAPI) with a username and a password.

7.1.3. SF.AUDIT

The TOE records and maintains security-related events in order to enable tracing of responsibilities for security-related acts and provides means to review the recorded data.

Thunder TPS scrubs traffic at multiple layers (hardware, layer 2/3, layer 4, layer 7), and violating of these checks are logged. DDoS Mitigation supports use of sFlow for collection and export of DDoS Mitigation statistics, at the modes Privileged EXEC level and configuration levels. Within sFlow records, the epoch timestamp in the header indicates when the samples were taken.

7.1.4. SF.PROTECTION

The TOE shall protect TSF data stored in the TOE from unauthorized exposure, modification and deletion.

Violating of hardware and software security checks shall be logged, and A10 Thunder TPS offers message logging management feature.

CLI commands for configuring and managing DDoS Mitigation features are organized in multiple levels, including User EXEC and Privileged EXEC for operational commands, where the administrator must be successfully logged on by means of username and password.

The User EXEC level can only make use of ping and some show commands.

The DDoS Mitigation tables and features shall only be managed by the Privileged EXEC administrator, because only the Privileged EXEC management level can employ commands for file management, clearing of DDoS information and configuration, together with all show commands. The Privileged EXEC administrator thus has the rights to modify and configure DDoS Mitigation rules, configure protection against DSN/HTTP/SSL/TCP/UDP-based attacks, clear entries from the DDoS Mitigation IP tables, and clear entries from the DDoS statistics.

A10 Thunder TPS also employs a GUI and the aXAPI open RESTful API for configuring and managing DDoS Mitigation features. The GUI and aXAPI support a single management level, described in the following:

- Privileged EXEC – As with this level when accessing via the CLI, supports the full set of management operations available.

GUI and aXAPI access for the Privileged EXEC level involves logging in (GUI) or authenticating (aXAPI) with a username and a password.

7.1.5. SF.INTEGRITY

The TOE ensures the integrity of system data.

Only the Privileged EXEC management level can employ commands for clearing of DDoS information. DDoS Mitigation tables, used to track the security status for traffic flows, shall only be configured by the Privileged EXEC administrator. ACOS begins creating dynamic DDoS Mitigation table entries for traffic as soon as the administrator enables DDoS Mitigation. To ensure that static entries are correctly used, the administrator should clear the dynamic entries from the DDoS Mitigation tables, after creating the static entries. This will clear any conflicting entries that would otherwise continue to be used instead of the static entries. Static entries are created when the administrator configure a DDoS Mitigation rule for a specific IP host, subnet, or geolocation. Static entries do not age out, and remain on the table unless the administrator clears the table.

Additionally, ACOS provides a redundancy feature allowing the administrator to stage a second Thunder TPS device as a standby in case the primary device becomes unavailable. If the Active device does become unavailable, ACOS fails over to the Standby device and resumes DDoS Mitigation operation.

7.1.6. SF.MANAGEMENT

The TOE provides means for the authorized administrator of the TOE to efficiently manage the TOE in a secure manner.

The TOE manages message logging, email alert notification and port mirroring. When DDoS Mitigation is enabled, the Privileged EXEC administrator can alter features and table information. If logging is configured, the over-limit event is also logged and can be read.

The administrator manages the Thunder TPS system mainly at two access levels, where the User EXEC level cannot alter any TSF data by use of the basic operation commands. The other access level is Privileged EXEC, at where the administrator can alter TSF data by several configuration operations. The User EXEC level can only perform basic operational commands, including ping and some show commands. The Privileged EXEC level can perform more extensive set of operational commands, including file management commands, clear commands, all show commands, and the configuration level commands, including global configuration, routing configuration, Interface configuration, GLID (rate limit) configuration, and DDoS Mitigation configuration.

When DDoS Mitigation is enabled, the feature automatically performs a fixed set of checks in hardware for all inbound traffic. For traffic that passes all these initial checks, additional checks are performed in software, based on the default limits or configured DDoS Mitigation rules.

7.1.7. SF.TESTS

DDoS Mitigation configurable rate intervals are tested.

DDoS Mitigation thresholds are calculated based on regular intervals. By default, each interval is one-tenth of a second long (0.1 seconds). Optionally, the administrator can set the rate interval to one full second instead. The one-second rate interval is helpful for testing the feature, since much less traffic is required to exceed the same configured thresholds. Using the one-second rate interval, DDoS Mitigation rate limits can be exceeded by only a tenth of the traffic required to exceed the same limits using the tenth-of-a-second rate interval.

Additionally, Tap mode deployment is useful for testing DDoS Mitigation features, or for sampling and exporting DDoS Mitigation data.