

可编程能力在新一代 安全设备中的重要性

通过基于软件的防火墙部署网络安全的传统方法，由于无法满足时延与带宽需求而无法扩展。将赛灵思自适应器件的灵活性及可配置性及其 IP 和工具产品相结合，能够显著提高安全处理性能。

概要

本白皮书探讨了多种防火墙架构，其中包括基于软件与 NPU 的架构，并且阐明了为什么新一代设计需要基于赛灵思自适应器件的内联防火墙架构。赛灵思 16nm FPGA 与 SoC 以及 7nm Versal™ ACAP 能够以硬化块与软 IP 的形式提供多种架构组件，因此使其成为设计新一代安全设备的理想选择。这些 IP 包括高速 SerDes 和多速率接口 IP，例如硬化 MAC、PCIe® 接口与存储器控制器。此外，赛灵思器件还可以提供具备流分类软搜索 IP 的业界一流存储器架构，使其成为网络安全和防火墙应用的最佳选择。

介绍

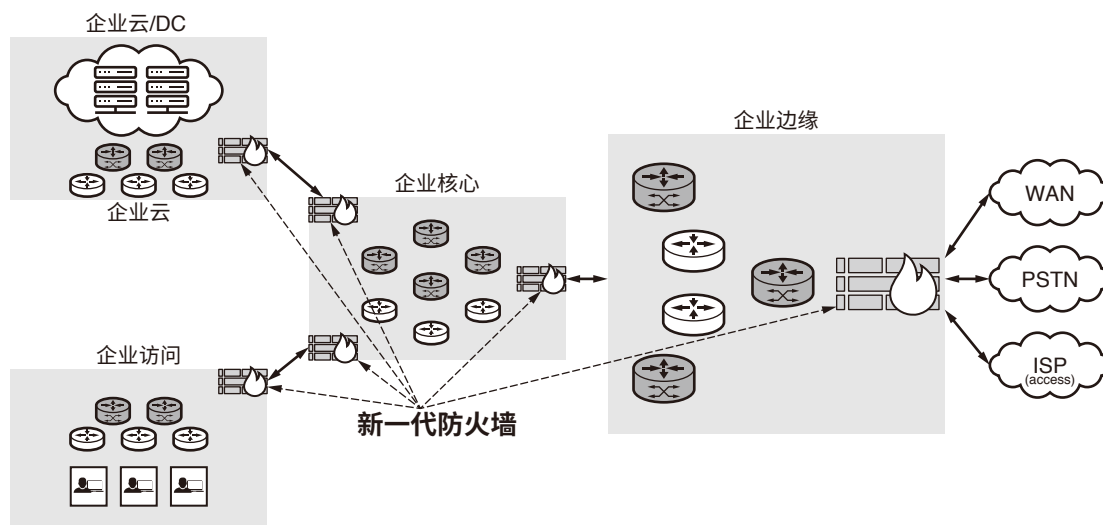
本白皮书介绍了在企业与电信数据中心网络中用作新一代防火墙 (NGFW) 的安全设备的功能、部署与架构。赛灵思器件的灵活性与可配置性与其 IP 与工具产品相结合，能够显著提高用于威胁检测与预防的网络安全设备的性能，同时可以实现性能扩展。此外，这些器件还可以助力实现即将面世的新一代安全技术，例如后量子加密 (PQC) 以及用于异常检测的机器学习 (ML) 技术。

由于企业网络正在向基于策略与意图的网络转型，因此流与策略可以定义有关流量的操作（路由、QoS、抛弃、标记等）。此外，输入流量所需的安全策略会根据网络中流的性质不断变化。大多数流量需要根据状态以动态方式处理网络流量。

基于端口的传统防火墙可以提供基于边界的保护，它可以根据数据包参数（如：IP 地址与 TCP/UDP 端口号）过滤流量，因为应用感知仅在软件中进行处理，其无法进行性能扩展。NGFW 应当不但能够识别和处理特定类别的流量，而且还应当能够识别与应用内容相关的威胁。企业使用的众多应用允许端口跳变，采用非标准端口或者隐藏 SSL 隧道中的威胁，因此传统的基于静态端口的防火墙无法检测出威胁与恶意软件。

企业网络防火墙

为确保企业办公室之间的安全性，历代网络防火墙都部署在网络边缘，其联网络采用多种传输网技术，而且往往会采用同一个网络流水线作为公共网。随着基于策略的网络的演进发展以及软件定义网络 (SDN) 与基于意图的网络 (IBN) 的涌现，具有不同吞吐量与功能的防火墙在逐步部署到企业网络的众多不同位置。参见图 1。



WP526_01_112920

图 1: 企业网络的新一代防火墙

如图 1 所示，防火墙的作用已经从企业网边界扩展到企业中的多个位置，如：连接企业总部与分支机构，保护连接边缘，或保护企业数据中心的流量不受企业访问的影响。NGFW 能够根据多种数据包参数（端口、IP 地址、有效载荷内容）或者根据 L3-VPN 或 SSL/TLS 等加密技术检测和阻止网段之间的威胁与恶意软件。

防火墙部署与功能

安全设备负责检查和分析来自企业网络外部的所有流量。防火墙能够部署到企业网络的多个位置，如：企业不同部门之间的流量，或者通过由交换机和路由器组成的多个网络节点从企业访问进入企业数据中心的流量。

安全设备 (NGFW) 可以内联部署，也能够以旁路模式部署。这两种模式的主要区别是内联模式直接连接到外部网络端口，而旁路设备可以连接到交换机或路由器的分流器或镜像端口。图 2 显示了网络中的防火墙连接。虽然防火墙的功能大同小异，但是内联防火墙比旁路防火墙设备更复杂，同时性能也更强大。

部署到具体位置的防火墙的规模与功能在策略规则分配方面有所不同，但是某些基本功能（如：流量分类、缓冲等）保持不变。

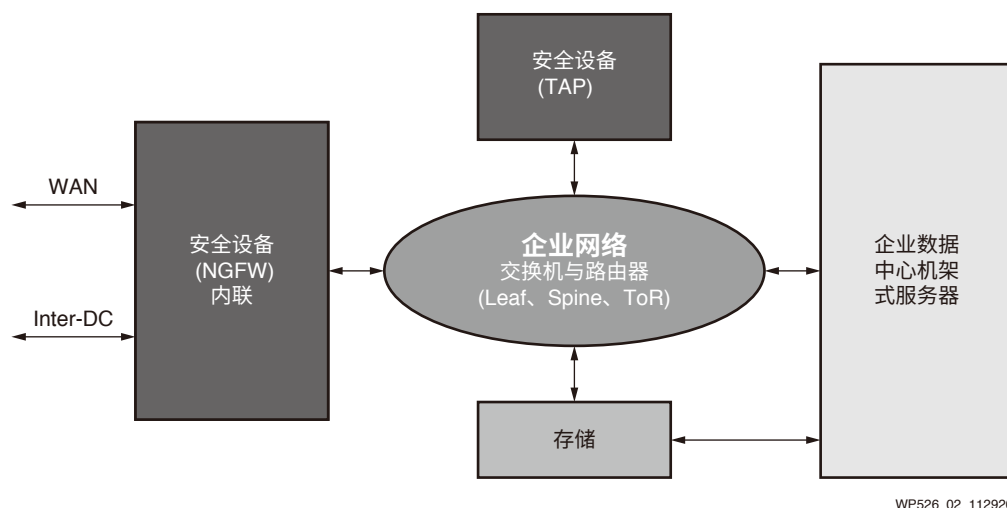


图 2：企业的网中的 NGFW

网络节点或安全设备可以负责实现以下安全功能：

1. L2 安全 - 用于链路加密的 MACSec
2. L3 安全 - 来自用户与其他网络节点的 VPN 隧道
3. 无效流量的阻断与过滤（基于协议与端口的过滤）
4. 传入与传流量的 TLS/SSL 加密/解密
5. 跨多个流量的异常检测
6. 状态模式匹配
7. 统计异常检测
8. IP 分片
9. TCP 重组与排序
10. 基于正则表达式 (regex) 的签名/内容匹配

除了上述功能之外，新一代网络安全产品也已经开始实现用于网络分析与恶意软件预测的 ML 模型。此类模型不依赖基于签名的传统检测功能。支持 ML 的防火墙可以收集遥测数据，而且可以在威胁出现之前提前部署安全策略。

上述功能的其中一部分是基本功能，是所有网络节点（安全交换机与路由器）的组成部分，而且是在采用 ASIC 或可编程器件创建的已部署网络交换机和路由器中实现；其他功能（L3 及更高级功能）更加复杂，需要大量流量分类与处理操作。网络协议层越高，流量处理的复杂性就越高。例如，层1(L1) 安全只需要帧级加密（如：OTN 传输有效载荷帧），而且是采用批量加密协议 (AES-GCM) 在光网络节点中实现。层 2(L2) 与层 3(L3) 需要在以太网与 IP 层面进行数据包处理，其需要数据包级别的处理。层 4(L4) 与更高级别

需要进行内容级安全处理，其中每个 TCP 或 UDP 会话都包括多个以太网与 IP 数据包。一些 L2 与 L3 安全功能可以在硬件器件（ASIC、ASSP、FPGA、SoC、ACAP 与 NPU）中轻松实现。此外，更高层的安全处理（L3 及以上）也需要对传入流量进行基于软件的内容处理，才能实现威胁检测与清除。

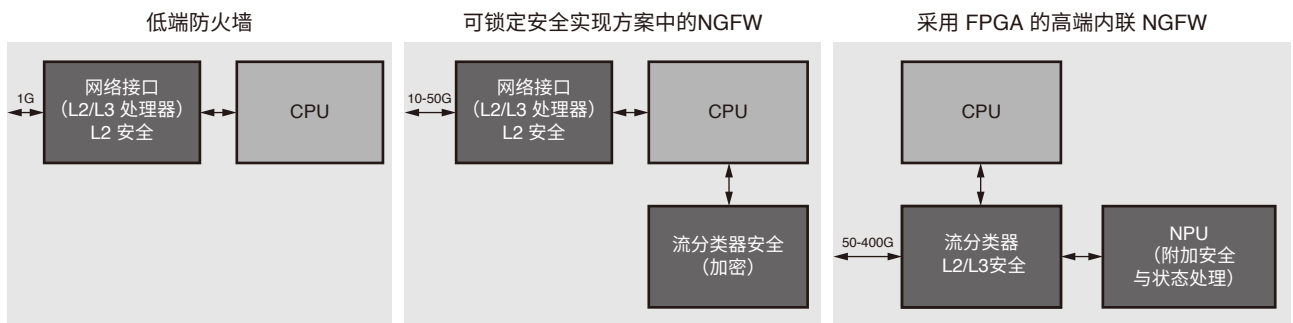
由于新的接入网技术（5G 前传、PON 与电缆）在过去几年已经大幅提高了吞吐量与流量，因此仅仅基于软件流量处理的防火墙设备不足以满足预期吞吐量下的性能与时延要求。

新一代防火墙的硬件架构

由于防火墙需要处理和检查所有的传入流量，因此它们需要执行以下操作：

- L2/L3 数据包处理
- L2/L3 安全功能
 - LinkSec/MACSec
 - L3-VPN/IPSec
- L4-L7 数据包处理与安全

图 3 显示为防火墙设计选项。



WP526_03_120220

图 3：防火墙的演进发展：旁路与内联处理对比

低端防火墙设备（通常低于 10G）的设计可以采用网络接口器件与 CPU。常见的网络接口（NIC）器件（定制 ASIC、FPGA 或 ASSP）可以处理处理传入流量（以太网与 IP 数据包），并且能够执行众所周知的 L2 与 L3 功能，而更高层（L4-L7）功能是由在 CPU 中运行的软件执行。

中端防火墙能够处理更高的吞吐量（10G-50G），其设计主要采用网络接口器件与旁路安全处理器（安全 ASIC、NPU 或 FPGA）。由于只使用软件的解决方案不能以更高的吞吐量对流量进行分类和处理，因此旁路安全处理器可以用作 CPU 协处理器，以便卸载加密/解密、公开密钥基础设施（PKI）和/或状态流量处理功能。虽然在这种架构中可以将 ASIC 或 NPU 用作网络接口，但是在中端防火墙中采用 FPGA 日渐流行，因为它在内联模式下可以实现处理传入流量所需的可扩展性和灵活性，从而可以降低威胁检测与预防方面的时延。

吞吐量达到 50G-400G 的新一代高端防火墙主要设计用于内联操作模式。在内联模式下，网络接口器件需要更加智能，才能处理庞大流量，这涉及到对传入和传出数据包的更深入的检查。此类接口器件也需要实现安全功能，如内联 IPSec，其采用常用的加密协议与 TCP 级安全。这种架构仍然采用 NPU 来实现具体的加密协议、PKI 和状态处理。内联设备的流量分类需求在流量数量与复杂性以及针对高吞吐量流量采取的措施方面各不相同。因此，用于内联安全处理的可编程器件（如 FPGA）是实现此类功能的理想选择。与 NPU 相比，FPGA 在流量处理方面提供了显著的时延降低和优异的可扩展性。此外，FPGA 目前还可以配置新一代存储器接口和片上高带宽存储器 (HBM)，这对于存储器密集型流量处理应用非常有用。

将 FPGA 用作网络安全的流量处理器

进出安全设备（防火墙）的流量进行多级别加密。L2 加密/解密 (MACSec) 是在链路层 (L2) 网络节点（交换机与路由器）进行处理。超出 L2（MAC 层）的处理通常包括更深层的解析、L3 隧道解密 (IPSec) 以及加密 SSL 流量与 TCP/UDP 流量的处理。数据包处理涉及传入数据包的解析与分类以及高吞吐量 (25–400Gb/s) 的庞大流量 (1–20M) 的处理。由于需要大量计算资源（核心），NPU 可以用于相对更高速率的数据包处理，但是无法实现低时延、高性能可扩展流量处理，因为流量处理采用 MIPS/RISC 核心，而根据其可用性来调度此类核心难度很大。采用基于 FPGA 的安全设备可以有效消除基于 CPU 和 NPU 的架构所带来的上述限制。

安全设备的流量处理

流量处理是数据包处理的更高级别的抽象，因为一个数据流是由类型相似的众多数据包组成。流量处理包括以下主要组成部分：

- 数据包解析
- 数据包查找
 - 路由查找
 - 根据数据包字段采用通配符搜索的流量查找
- 数据包编辑
 - 校验和计算
 - 包头封装/解封
 - 安全包头封装

赛灵思提供了采用高级抽象语言 P4 进行数据包处理的工具，其可以实现数据包解析、分类、查找与数据包编辑功能。与基于 RTL 语言的实现相比，使用 P4 完成数据包处理可以在更高的抽象层实现。采用 P4 可以提高现有可编程 FPGA 架构的灵活性，因为它可以轻松实现数据包解析、数据包编辑以及流量表条目的修改。

如图 4 所示，P4 介绍可以采用 P4 编译器编译的并且映射在赛灵思 FPGA 中的数据包处理流水线架构，其中采用了基本架构组件。P4 语言定义数据包解析、查找（IPv4、IPv6 和其他数据包字段）以及数据包的编辑（逆解析）。P4 定义的架构可以直接应用于安全处理流水线，如：IPSec 安全关联 (SA)、安全策略 (SP) 查找以及进/出流量的隧道处理实现。

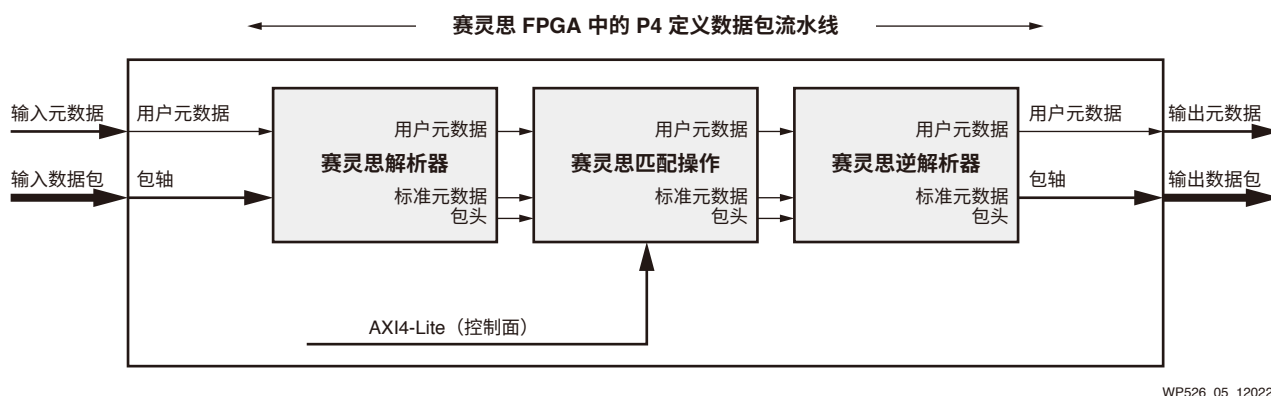


图 4：基于 P4 的数据包处理流量分类与查找

数据包处理的三个主要组成部分包括：

数据包解析：来自多个应用，访问企业网络与数据中心网络不同节点所产生的流量需要针对具体流量类型分类。解析过程涉及众多数据包参数的提取，其中包括 L2 包头、L3 包头以及来自数据包已知偏移量的字段。这些解析需求随应用不同以及数据包不同位置的签名不同而变化。FPGA 的灵活架构加上 P4 定义的解析器能够满足这些不断变化的分类需求。

数据包查找：

完成解析之后，需要根据流量的类型对数据包进行分类。加密的数据包根据协议与安全包头字段进行解密处理。

匹配操作模块对数据包解析器模块生成的搜索密钥进行查找，以实现目的地/操作分配。

对于加密流量，密钥搜索包括安全关联与安全策略的确定，它可以决定应用于加密数据包的解密密钥信息和策略。

L2 加密数据包 (MACSec) 需要更简单直接的查找，而更高层的加密查找可能更加复杂，具有更宽泛的密钥与结果值。

图 5 介绍了 MACSec、IPSec 和 TCP 协议的查找示例。查找次数随网络节点变化，不过某些情况下一些流量类别需要多层查找。

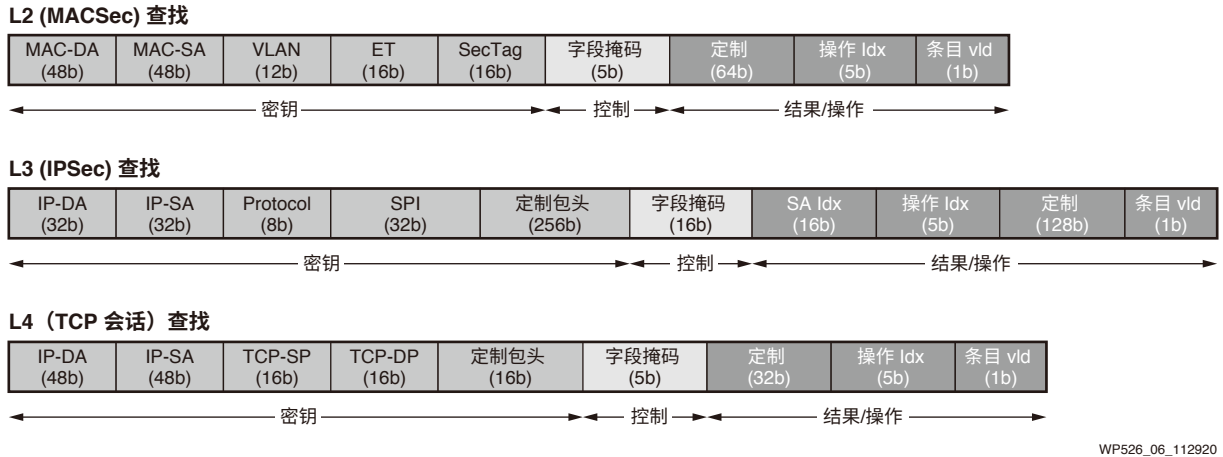


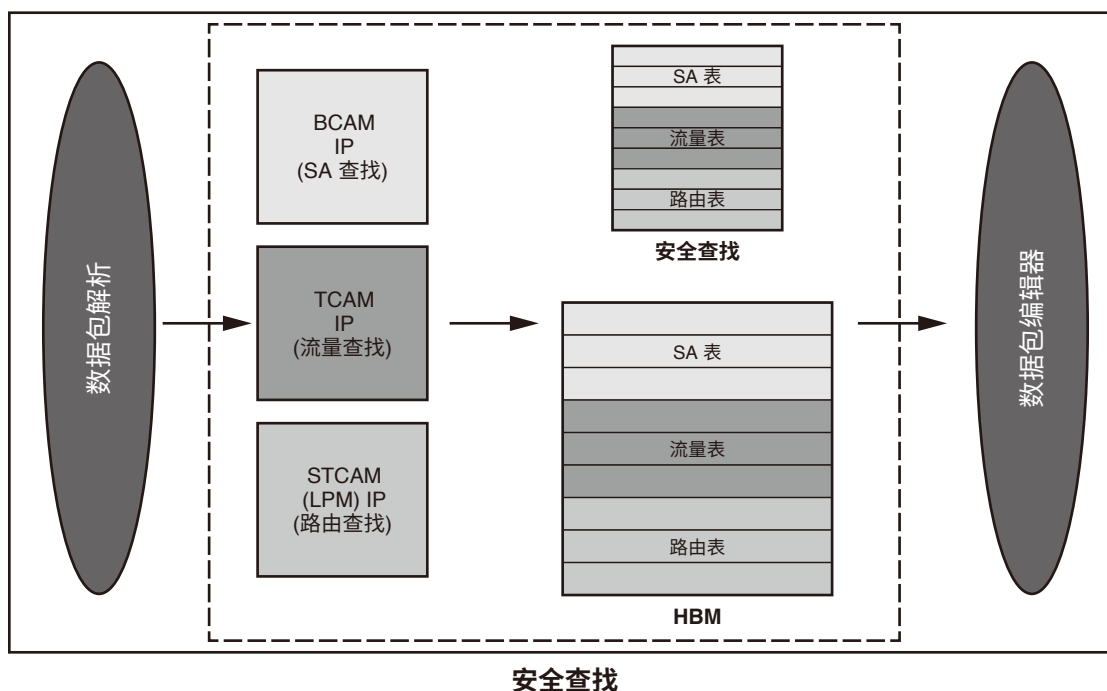
图 5: L2/L3/L4 安全实现方案查找示例

上述查找特定于安全处理。此外，防火墙也可以针对路由器功能、网络地址转换 (NAT) 以及传入流量的策略（或访问控制）查找实现附加查找。

以下安全与网络查找类别包括精确匹配、最长前缀匹配 (LPM) 和通配符搜索，其采用由包头字段组成的密钥：

- 路由查找
- NAT 查找
- 采用多个字段的流量分类

如图 6 所示，数据包处理查找可分为三类，有各自的表和密钥大小要求。



WP526_07_120220

图 6: 采用基于 FPGA 的安全设备进行查找

赛灵思的 IP 产品组合包括用于二进制匹配、通配符三元匹配和最长前缀匹配的搜索 IP。这些搜索 IP 可以灵活组合，以适应所有采用片上 SRAM 与 DRAM (HBM) 的赛灵思 FPGA。这三类搜索 IP 全部支持 100Mb/s 至 400Gb/s 吞吐量。

密钥宽度、结果宽度和表内的条目数量可以决定 FPGA 所用片上逻辑资源和存储器 (SRAM/DRAM) 的数量。由于赛灵思拥有具有不同资源（逻辑/存储器）数量的广泛器件类别，因此用户能够针对其吞吐量与表大小要求选择具有适当资源的赛灵思器件。此外，查找 IP 配备用于修改和更新流量表条目的应用层软件 API。

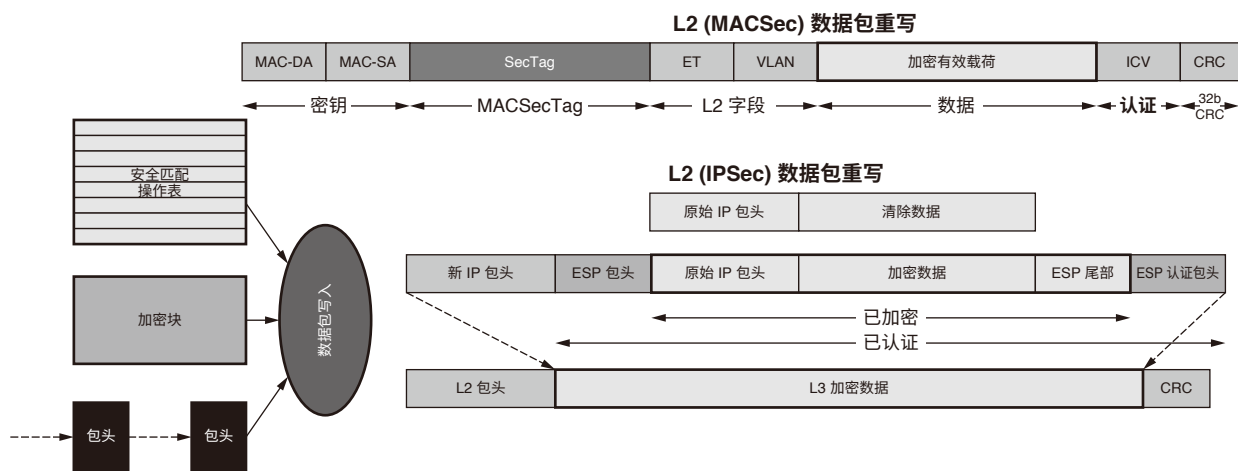
数据包编辑：

安全处理涉及在完成解析、包头查找和过滤之后将修改后的加密或解密数据包发送到出站端口。传出流量包括修改后的新包头、更新后的数据包字段、认证包头以及纠错字段。

部分常见数据包处理需求包括：

- 更改 L2/L3 包头 (MAC/VLAN/IPv4/IPv6)
- 创建与更新安全 (MACSec/IPSec) 包头
- 更新 IP 包头校验和
- 更新 TCP 校验和
- 更新以太网 CRC
- 更新认证字段

图 7 显示了用于 MACSec 和 IPSec 的数据包编辑/修改操作。在通过出站端口发送数据包之前，可能需要对包头字段进行多次修改，这包括校验和与 CRC 的计算与插入。除了标准包头，数据包通常还包括专用包头，而且也可能需要采用不同的协议包头（VXLAN、IP in IP、GRE 等）对数据包进行封装与解封。赛灵思可编程器件能够在线路速率下以最大灵活性实现数据包修改。



WP526_08_112920

图 7: MACSec 与 IPSec 数据包重写

此外，赛灵思器件还提供 P4 可编程能力，因此也可以采用 P4 实现数据包重写操作。与 RTL 实现方案相比，P4 逆解析器功能能够进一步简化包头的创建与插入。为在赛灵思器件上以线路速率运行，可以使用赛灵思 P4 编译器合成 P4 编辑器代码。

对于应用层安全实现，对数据包重写操作的需求更加复杂。例如，如果 TCP 数据包在 FPGA 内终止，则会话追踪与封装/解封需求会比 IPSec 或 MACSec 数据包修改需求需要更多的逻辑与存储器资源。

此外，数据包修改任务也可以在软件（运行 CPU 核心）中执行，但是高端安全设备所需的吞吐量无法通过软件实现方案满足线路速率操作。在可编程硬件中执行数据包处理操作的另一个关键优势是可以节省大量的 CPU 资源（CPU 核心），节省下来的资源可以分配给软件中运行的实际应用。

FPGA 中的应用级安全处理

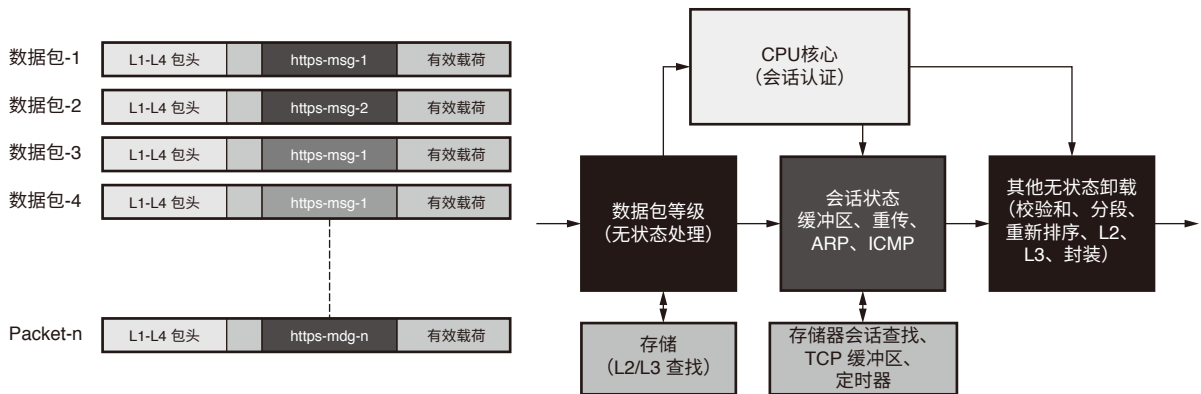
FPGA 是新一代防火墙内联安全处理的理想选择，这是因为采用 FPGA 可以成功满足对更高性能、灵活性和低时延操作的需求。此外，FPGA 还可以实现应用级安全功能，从而进一步节省计算资源并提高性能。

FPGA 中有关应用安全处理的常见示例包括：

- TCP 卸载引擎
- 正则表达式匹配
- 非对称加密 (PKI) 处理
- TLS 处理

由于众多用户空间应用采用 TCP 作为客户端或服务器模式下的通信协议，并且 TCP 是客户端与服务器之间的安全 (TLS/SSL) 连接基本块，因此 TCP 卸载引擎 (TOE) 是用于内联 FPGA 处理的重要卸载块。企业防火墙通常同时终止大量 TCP 连接，这将消耗大量的 CPU 周期与存储器。为了实现应用级安全处理，可能需要采用拥有大量核心的昂贵的高端 CPU 来终止众多 TCP/UDP 连接。FPGA 中的 TCP 处理实现方案通过节省众多实现 TOE 所需的内核，能够显著节约成本和功耗。

图 8 显示了安全设备中由 FPGA 辅助完成数据包处理的示例。由于进入防火墙网络接口的数据包可能属于众多不同的应用，因此追踪与多个应用关联的数据包，并将其发送到正确应用或者在正确应用进行接收是一种需要占用大量存储器的状态化操作。此外，上述关联还需要对 TCP 段进行重新排序、分段和重组。虽然仍然可以采用 CPU 处理协议消息的新连接请求与认证，但是 FPGA 可以追踪活动会话并且根据会话 ID 将数据包分配给相关应用。



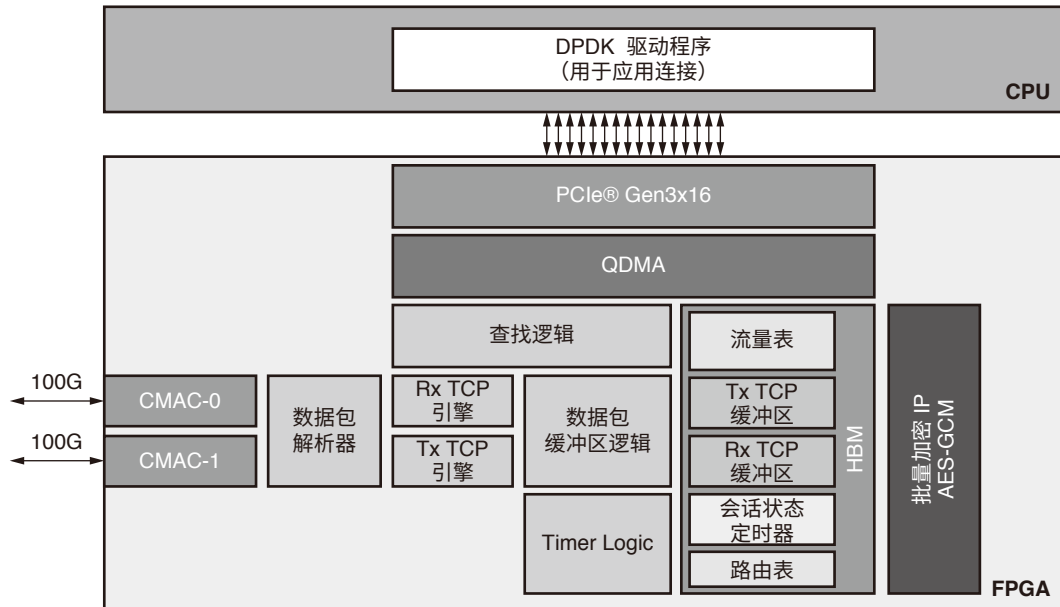
WP526_09_120420

图 8：采用 FPGA 进行应用级状态处理

FPGA 中的 TLS 卸载/处理

FPGA 的 TLS 处理功能是 TCP 卸载引擎的扩展，其中 TCP 有效载荷的加密与解密在 FPGA 中执行。TSL 会话的发起与认证在软件中执行 CPU)。在建立安全连接时，由 FPGA 执行后续的 TLS 记录处理。

图 9 显示了在赛灵思器件中作为 CPU 卸载的完整内联 SSL 处理功能的组件。赛灵思器件可以实现整个逻辑，以处理 100G 以太网接口数据包。它可以识别 TCP 与 TLS 流，并且相应地将数据包引导到相关 CPU 或者采用可编程资源进行处理。



WP526_10_120420

图 9: FPGA 中的 TLS 卸载

FPGA 中的正则表达式 (Regex)

正则表达式 (regex) 涉及流量的有效载荷数据中字符串或特殊字符的匹配。它广泛应用于 DPI、IPS/IDS、DLP 和 DDoS 防护。Regex 匹配通常是在软件中执行，其采用专用软件库。由于 regex 搜索需要针对众多规则对有效载荷进行匹配，因此纯软件 regex 处理给新一代安全设备带来了性能与时延挑战。

图 10 说明了采用赛灵思器件的 100Gb/s 内联 regex 处理。在此 regex 加速处理模型中，Perl 兼容正则表达式 (PCRE) 或 Snort 规则首先在软件编译器中进行编译，然后通过 PCI 接口发送到与 CPU 连接的 FPGA，作为二进制字符串匹配规则条目保存到 FPGA 的内部 SRAM 或 DRAM (HBM 或 DDR) 存储器。FPGA 会在内部 SRAM 或 DRAM (片上 HBM 或外部 DDR) 中填充大量 regex 规则/条目 (转换成二进制的特殊字符与字的组合)。regex 处理的内联加速与软件相比可以显著提高性能 (10-30 倍)。

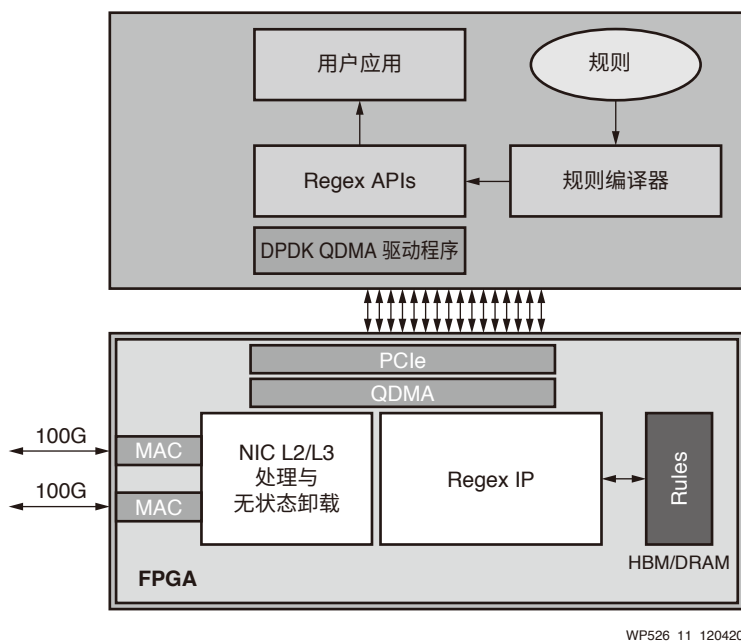


图 10: FPGA 中的 Regex 匹配

基于 FPGA 的安全设备中的机器学习 (ML)

在新一代安全设备中，基于 ML 的流量分析与恶意软件检测是关键应用之一。ML 模型将会被部署用于通过分析加密数据中的特定模式而实现的加密流量检测。在高端安全设备中，则需要采用 ML 模型处理海量实时数据，以便预测异常，因此采用加速器实现 ML 模型将给高吞吐量与低时延恶意软件预测带来巨大优势。防火墙已经开始在软件中部署用于异常检测的 ML 模型。在新一代设备中，赛灵思可编程器件将会通过将 ML 模型卸载到可编程逻辑而提供显著提高的预测速度。

此类基于 FPGA 的 ML 模型包括：

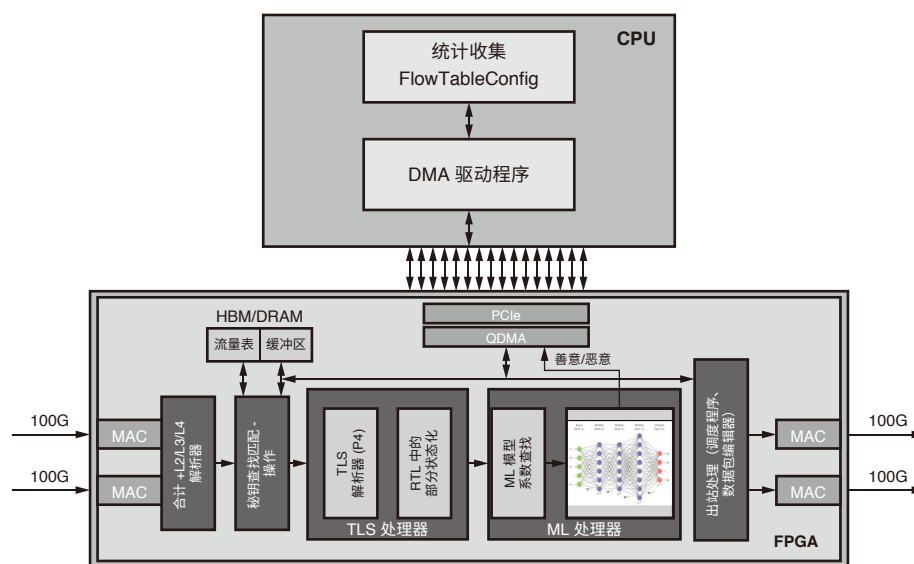
- 随机树 (随机森林)
- 深度神经网络 (DNN)
 - 多层感知机 (MLP) 或卷积神经网络 (CNN)

推断模型的选择取决于多种因素，如：准确性、输入模式改变频率、训练需求、FPGA 资源利用率等。

赛灵思 ML 解决方案包括支持大多数常用 ML 框架的软件库与工具。这些模型可以高效映射到赛灵思可编程器件以及 Versal ACAP 所提供的 AI 引擎中的查找表 (LUT)、DSP 与 SRAM/DRAM 存储器。

针对 FPGA 中安全分析功能实现 ML 模型的另一个优势是恶意软件预测所需要的内联流量/数据包处理可以在同一个 FPGA 中执行。在 ML 模型的内联实现方案中，将网络接口连接到同一个 FPGA 可以节省从 CPU 向 ML 模型发送数据所需的 PCIe® 带宽。

图 11 显示了 ML 模型在 200Gb/s 防火墙中的应用。TLS 处理器具有 TSL 解析器以及 IP 数据报中 TLS 参数提取功能。随后，这些参数反馈给 ML<5018/> 处理器，以便查找和调节 ML 模型的系数。根据相关系数，模型可以预测 TSL 流量的善意与恶意签名。



WP526_12_112920

图 11: 安全设备中的 ML 模型

采用 FPGA 的新一代安全技术

后量子加密

众多现有的非对称算法容易受到量子计算机的破坏。对量子计算安全加密算法的研究和实现已经起步，而已经有学术论文介绍了如何采用 FPGA 实现此类算法。RSA-2K、RSA-4K、ECC-256、DH 和 ECCDH 等非对称安全算法受到量子计算技术的影响最大。目前正在探讨新的非对称算法实现方案和 NIST 标准化。

目前提议的后量子加密 (PQC) 包括针对以下方面的环上误差学习 (R- LWE) 算法：

- 公共密钥加密 (PKC)
- 数字签名
- 密钥创建

提议的公共密钥加密的实现方案包括某些众所周知的数学运算（TRNG、高斯噪声采样器、多项式加法、二进制多项式定标器除法、乘法等）。用于众多此类算法的 FPGA IP 已经面世或者可以采用 FPGA 构建块高效实现，如：现有的和新一代赛灵思器件中的 DSP 与 AI 引擎。

安全访问服务边缘 (SASE)

安全访问服务边缘 (SASE) 是新兴的新一代企业安全技术，旨在满足企业的动态安全访问需求。SASE 的早期定义在企业边缘集成自适应网络与安全需求，其中包括 SD-WAN、软件与物理防火墙以及网络安全网关。SASE 需要采用动态安全策略更新来提供对联网应用的不间断安全访问。

采用 FPGA 在硬件中实现 SASE 刚刚起步，不过，由于 FPGA 具有全面的可编程能力，因此它们仍然能够通过 L2/L3/L4 加密技术和上述其他技术在流量处理以及动态安全连接流水线的提供方面起到重要作用。

用于安全设备的赛灵思工具与 IP

赛灵思器件具有高性能可编程资源以及业界一流的工具与 IP，是设计和实现网络流量安全处理的理想选择。它们可以提供最高数据与信号处理能力，以及最新的多速率高吞吐能力。SerDes 用于符合最新接口标准的设计，其中包括 1G-400G 以太网、600G Interlaken 以及高达 400G PCIe 吞吐量。此外，赛灵思器件还提供注册裸片间路由线路，可支持高达 600MHz 可编程逻辑运算。

除了基本的高性能设计资源，赛灵思还提供用于安全处理的多种设计 IP。这些可编程 IP 包括 MAC 接口、用于向/从主机传输数据的高速 DMA、用于流量分类与路由的搜索 IP（BCAM、TCAM 与 STCAM）以及使用 AES-GCM 密码进行批量加密的片上 HBM 和/或 DDR 存储器接口与软加密引擎 (SCE)。

此外，赛灵思还拥有合作伙伴生态系统，其可以提供采用多种密码协议的批量加密端到端解决方案，以及使用大多数常见密钥交换（ECCDH、RSA-2K、RSA-4K 等）进行非对称加密的 IP。除了来自合作伙伴的基础级标准加密 IP 之外，赛灵思目前还在与合作伙伴合作实现高级 (L4+) 安全 IP，其中包括：

- 带有大量活动会话的 TCP 卸载引擎
- 内联 SSL 卸载参考设计
- 应用级安全卸载（5G L2 加速）
- 10K+ IPSec 会话数据包处理

赛灵思的最新器件 (Versal™ Premium ACAP) 配备有硬化高速加密引擎 (HSC)，可用作加密引擎，实现基于 AES-GCM 协议的高达 400Gb/s 的 MACSec、IPSec 或 SSL 处理。每个 HSC 引擎都能够以 1x400G、2x200G 或 4x100G 通道化模式支持 MACSec、IPSec 和任何其他批量加密需求，每 100G 最多支持 128 个安全关联 (SA)。采用可编程逻辑可以实现其他 SA。

总结

由于通信网络（边缘、接入和核心网）正在向具有应用级政策感知功能的更高性能转型，对更高吞吐量的安全处理的需求已经大幅增加。此外，随着接入技术的升级以及 5G 接入技术 (xHaul)、新一代 PON 和有线网络的部署，接入网络的设备数量会以指数方式增长。新一代网络安全设备需要具备 2~4 倍吞吐量，用于 L2 (MACSec) 安全与 L3 (IPSec) 安全处理。此外，新一代网络会更多依赖意图与策略，因此对高吞吐量应用级安全处理 (L4-L7 安全) 的需求已经显著增加。

高吞吐量应用安全实现方案需要高吞吐量数据包处理，以及用于加密需求的大量计算资源。纯软件应用安全实现方案无法满足对性能与时延的期望。对于 5G 低时延应用来说，时延需求更加重要，因此，采用可编程加速器作为内联安全处理器在新一代安全设备中的重要性日益突出。

在新一代防火墙中采用赛灵思器件不仅可以解决吞吐量和时延问题，其他优势还包括助力新技术的实现，如：机器学习 (ML) 模型、安全访问服务边缘 (SASE) 和后量子加密 (PQC)。赛灵思器件可以为面向这些技术的硬件加速提供理想平台，因为仅用软件实现方案无法满足性能需求。赛灵思正在针对现有的和新一代网络安全解决方案不断开发和升级 IP、工具、软件以及参考设计。

鸣谢

以下赛灵思员工对本白皮书的撰写做出了贡献：
首席架构师兼技术营销总监 *Awanish Verma*。

修订历史

下表列出了本文档的修订历史：

日期	版本	修订描述
2021年 3 月 22 日	1.0	赛灵思初始版本。

免责声明

本文向贵司/您所提供的信息（下称“资料”）仅在对赛灵思产品进行选择和使用参考。在适用法律允许的最大范围内：(1) 资料均按“现状”提供，且不保证不存在任何瑕疵，赛灵思在此声明对资料及其状况不作任何保证或担保，无论是明示、暗示还是法定的保证，包括但不限于对适销性、非侵权性或任何特定用途的适用性的保证；且 (2) 赛灵思对任何因资料发生的或与资料有关的（含对资料的使用）任何损失或赔偿（包括任何直接、间接、特殊、附带或连带损失或赔偿，如数据、利润、商誉的损失或任何因第三方行为造成的任何类型的损失或赔偿），均不承担责任，不论该等损失或者赔偿是何种类或性质，也不论是基于合同、侵权、过失或是其他责任认定原理，即便该损失或赔偿可以合理预见或赛灵思事前被告知有发生该损失或赔偿的可能。赛灵思无义务纠正资料中包含的任何错误，也无义务对资料或产品说明书发生的更新进行通知。未经赛灵思公司的事先书面许可，贵司/您不得复制、修改、分发或公开展示本资料。部分产品受赛灵思有限保证条款的约束，请参阅赛灵思销售条款：<http://china.xilinx.com/legal.htm#tos>；IP 核可能受赛灵思向贵司/您签发的许可证中所包含的保证与支持条款的约束。赛灵思产品并非为故障安全保护目的而设计，也不具备此故障安全保护功能，不能用于任何需要专门故障安全保护性能的用途。如果把赛灵思产品应用于此类特殊用途，贵司/您将自行承担风险和责任。请参阅赛灵思销售条款：china.xilinx.com/legal.htm#tos。

关于与汽车相关用途的免责声明

如将汽车产品（部件编号中含“XA”字样）用于部署安全气囊或用于影响车辆控制的应用（“安全应用”），除非有符合 ISO 26262 汽车安全标准的安全概念或冗余特性（“安全设计”），否则不在质保范围内。客户应在使用或分销任何包含产品的系统之前为了安全的目的全面地测试此类系统。在未采用安全设计的条件下将产品用于安全应用的所有风险，由客户自行承担，并且仅在适用的法律法规对产品责任另有规定的情况下，适用该等法律法规的规定。