RdS
RICERCA DI SISTEMA

ENEA
AGENZIA NAZIONALE PER LE NUOVE TECNOLOGIE, L'ENERGIA E LO SVILUPPO ECONOMICO SOSTENIBILE

MINISTERO DELL'AMBIENTE E DELLA SICUREZZA ENERGETICA

Ricerca di Sistema elettrico

Definizione dei requisiti di una infrastruttura di calcolo HPC a basso consumo per il controllo informatico di reti intelligenti cyber-resilienti (LA3.2)

Paolo Palazzari, Luigi Acampora, Salvatore Pecoraro

RdS_PTR 22-24_PR 2.1_LA3.2_068

DEFINIZIONE DEI REQUISITI DI UNA INFRASTRUTTURA DI CALCOLO HPC A BASSO CONSUMO PER IL CONTROLLO INFORMATICO DI RETI INTELLIGENTI CYBER-RESILIENTI (LA3.2)

Paolo Palazzari, Luigi Acampora, Salvatore Pecoraro (ENEA-ICT-RETE)

Giugno 2023

Report Ricerca di Sistema Elettrico

Accordo di Programma Ministero dell'Ambiente e della Sicurezza Energetica - ENEA
Piano Triennale di Realizzazione 2022-2024

Obiettivo: *Decarbonizzazione/Digitalizzazione ed evoluzione delle reti*
Progetto: *Tema di ricerca 2.1, Progetto integrato cyber security dei sistemi energetici*
Linea di attività: *LA3.2*
Responsabile del Progetto: Maria Valenti, ENEA
Responsabile Linea di Attività: Paolo Palazzari, ENEA
Mese inizio previsto: M1
Mese inizio effettivo: M1
Mese fine previsto: M18
Mese fine effettivo: M18

Indice

1 Risultati attesi

Lista dei risultati attesi come da capitolato vigente

Si riporta di seguito la lista dei risultati attesi come da capitolato vigente:

- Dettagli inerenti ai requisiti di un'infrastruttura di calcolo a basso consumo HPC per reti cyber-resilienti;
- Descrizione dettagliata dell'infrastruttura di calcolo in cui saranno specificati: dispositivi programmabili (con le relative toolchain SW) adottati per implementare gli algoritmi di criptazione; dispositivi di controllo periferici, basati su AI, che garantiranno la sicurezza rispetto agli attacchi esterni; schede di calcolo che costituiranno i nodi della infrastruttura; sensori presenti nell'infrastruttura e la relativa modalità di collegamento.

2 Risultati ottenuti

Lista dei risultati ottenuti *(Evidenziare in che misura il risultato è stato ottenuto ed il beneficio per il sistema elettrico nazionale e i suoi utenti. Aggiungere eventuali risultati ottenuti non previsti nel capitolato)*

Di seguito è riportato l'elenco dei risultati ottenuti:

- **Dettagli inerenti ai requisiti di un'infrastruttura di calcolo a basso consumo HPC per reti cyber-resilienti**

  Come previsto dal capitolato, è stata definita l'architettura HW/SW della infrastruttura di calcolo HPC a basso consumo per il controllo informatico di reti intelligenti cyber-resilienti.

  Un'infrastruttura HPC con acceleratori FPGA per il controllo delle reti intelligenti cyber-resilienti è un asset prezioso per il sistema elettrico nazionale e i suoi utenti. Per prima cosa, consente una gestione efficiente delle reti intelligenti, ottimizzando la distribuzione e il consumo di energia. Inoltre, può reagire istantaneamente a emergenze come guasti o attacchi informatici, garantendo un servizio continuo e sicuro. Grazie agli acceleratori FPGA, è possibile sviluppare soluzioni di difesa cibernetica avanzate, rendendo il sistema resiliente alle minacce digitali. L'analisi dei dati storici e in tempo reale aiuta a prevedere la domanda energetica futura, riducendo gli sprechi e migliorando l'efficienza complessiva. In breve, questa infrastruttura non solo migliora la gestione energetica, ma anche la sicurezza e l'affidabilità del servizio elettrico per tutti gli utenti, rappresentando un investimento essenziale nell'evoluzione del settore energetico.

- **Descrizione dettagliata dell'infrastruttura di calcolo**

  È stata fornita una descrizione dettagliata dell'infrastruttura di calcolo comprendente i seguenti elementi: dispositivi programmabili (con le relative toolchain SW) adottati per implementare gli algoritmi di criptazione; dispositivi di controllo periferici, basati su AI, che garantiranno la sicurezza rispetto agli attacchi esterni; schede di calcolo che costituiranno i nodi della infrastruttura; sensori presenti nell'infrastruttura e la relativa modalità di collegamento.

3 Prodotti attesi

Lista dei prodotti hardware/software eventualmente attesi per la LA.

La LA3.2 non prevede lo sviluppo di prodotti hardware/software.

4 Prodotti sviluppati

Lista dei prodotti hardware/software eventualmente sviluppati nella LA, illustrando, per il software, le modalità di accesso per gli utenti *(Aggiungere eventuali prodotti sviluppati non previsti nel capitolato)*

La LA3.2 non prevede lo sviluppo di prodotti hardware/software.

5 Analisi degli scostamenti su attività e risultati

(8000 caratteri max)
Descrivere le motivazioni di eventuali scostamenti tecnici/economici rispetto al preventivo e criticità riscontrate (*Evidenziare il contenuto in riferimento al piano di rischi presentato*)

La LA non ha presentato scostamenti di natura tecnica e ha raggiunto tutti gli obiettivi prefissati. Si segnala, però, che è stato richiesto il coinvolgimento di 1 profilo tecnico a supporto delle attività di ricerca. In particolare, il personale tecnico ha contribuito alla progettazione collaborando nell'analisi dei requisiti che sono necessari per la selezione dell'hardware, della configurazione delle reti e la progettazione di architetture di archiviazione scalabili, tenendo conto delle configurazioni hardware e software già presenti nell'ambiente di calcolo e reti ENEA.

6 Sintesi delle attività svolte

(1000 caratteri max)

Si è definita l'architettura HPC e ne sono stati selezionati i componenti. Linee guida adottate:

- Acquisire componenti allo stato dell'arte (acceleratori, server, firewall, sensoristica).
- Configurare un'architettura di calcolo innovativa. L'innovatività non risiede nelle singole componenti dell'architettura ma nell'impiego congiunto di tali metodiche / tecnologie. Al momento non ci risulta che esistano architetture simili.
- Adottare uno stack SW che integri l'architettura di calcolo nella rete del centro ENEA Casaccia, per assicurare l'inter-esistenza della rete progettata con la rete dati preesistente, che fornisce servizi che dovranno continuare ad esistere, integrando le funzionalità introdotte dalla nuova architettura.

- La rete di calcolo / comunicazione costituirà un asset importante per il sistema energetico, che potrà impiegare l'architettura HPC come struttura per gestire la sensoristica e le necessità di processamento e comunicazione previste dal sistema energetico.

7 Dettaglio delle attività svolte

(15000 caratteri max)
Descrivere in dettaglio le attività svolte nella LA (*Evidenziare come si sono ottenuti i risultati. Descrivere brevemente anche le attività, per le quali si sono spese delle risorse, che tuttavia non hanno portato all'ottenimento dei risultati previsti al fine di permettere la corretta valutazione di congruità e pertinenza dei costi rendicontati.*)

In questa prima fase del progetto si è proceduto a definire l'architettura dell'infrastruttura di calcolo HPC da realizzare per creare un ambiente cyber-resiliente, in grado di interagire in maniera sicura con reti di sensori/attuatori, creando dei log dei dati di interesse. Siccome questa infrastruttura è dedicata al sistema energetico, i sensori/attuatori selezionati per la realizzazione prototipale sono degli smart-meters che permettono di monitorare i valori di tensione e corrente (oltre che la temperatura ambiente) di diverse prese.

Le attività svolte hanno visto il coinvolgimento della Divisione ICT e dei Laboratori HPC e Reti dell'ENEA, che hanno lavorato alla definizione dei requisiti dell'architettura di calcolo in continuo confronto con le Università Roma3 e "La Sapienza", co-beneficiarie del progetto. Il coinvolgimento di esperti di vari domini (calcolo, reti, database, cifratura, cybersecurity e AI) e di aziende fornitrici degli apparati di rete, storage e calcolo e sensoristica dei vari settori, ha permesso, inoltre, una analisi approfondita dei requisiti delle singole componenti dell'infrastruttura garantendo la compatibilità con l'infrastruttura HW/SW preesistente e, al contempo, il soddisfacimento delle esigenze di sicurezza e di prestazioni richieste.

Le attività sono state relative alla progettazione dell'architettura dell'infrastruttura, come riportato di seguito.

L'infrastruttura di calcolo HPC a basso consumo per il controllo informatico di reti intelligenti cyber-resilienti, deve essere in grado di

1- Dialogare con sensori ed attuatori in maniera sicura
2- Creare dei log dei dati rilevanti, opportunamente selezionabili
3- Proteggere i nodi interni da possibili attacchi esterni
4- Mettere a disposizione dispositivi di elaborazione a ridotto consumo energetico

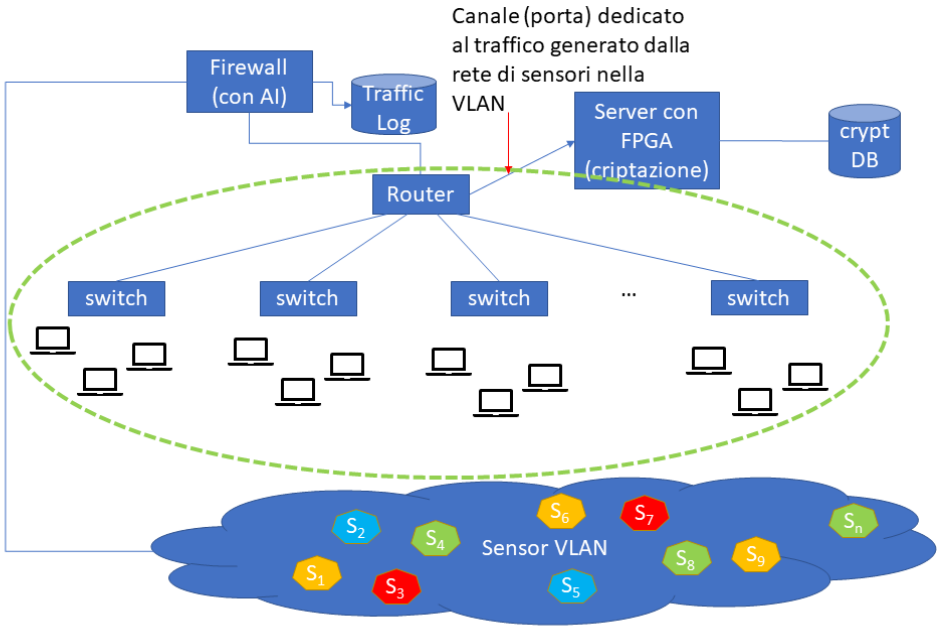

Fig. 1: schema di principio dell'infrastruttura di calcolo HPC

In Figura 1 si riporta lo schema che verrà adottato per implementare la infrastruttura di calcolo HPC. La parte interna all'area tratteggiata rappresenta la rete di campus attualmente presente nel centro ENEA Casaccia. Ci sono varie sottoreti (corrispondenti ai vari edifici del campus), collegate ad un router/gateway che permette la connettività interna e fornisce l'accesso alla rete internet. La rete di sensori/attuatori, distribuita nel campus, sarà realizzata come una VLAN. La sicurezza delle comunicazioni nella sensor VLAN sarà garantita tramite il Firewall PA-3260, dotato di avanzate funzionalità di AI: grazie a queste, il firewall è in grado di riconoscere la tipologia di traffico IoT e, nel caso dovesse rilevare pattern di traffico non riconducibili all' IoT, può intervenire bloccando i messaggi potenzialmente pericolosi. La sensor VLAN sarà accessibile solamente dai nodi di calcolo autorizzati dal Firewall, come ad esempio il nodo equipaggiato con schede FPGA e preposto all'implementazione di algoritmi di crittazione per lo storage dei dati provenienti dalla sensor VLAN.

I canali di comunicazione della VLAN rispecchiano le caratteristiche dei canali fisici cui si appoggiano e sono dell'ordine del Gb/s per i canali interni agli switch e dei 10 Gb/s per i canali di up-link degli switch.

Per implementare gli algoritmi di crittazione tramite i quali proteggere i dati provenienti dalla sensor VLAN prima di memorizzarli all'interno di un Data base, si è deciso di utilizzare le schede Alveo U280 della Xilinx (AMD). Tale scelta è motivata:

- dall'elevata quantità di risorse disponibili nelle FPGA XCU280 ospitata in questa scheda, basata sull'architettura UltraScale+ a 16 nm. Tale FPGA ha 1.3 milioni di look-up tables (6 bit di ingresso, 1 bit di uscita), 9024 DSP, 1490 block RAM (36 Kb) e 960 UltraRAM (288 Kb). Tali risorse permettono di avere una banda aggregata interna di memoria di 35 TB/s
- dal contenuto assorbimento di potenza (tipico TDP = 100W, max TDP=225W)

- dalla presenza di un core PCIe Gen3x16 / Gen4x8, che consente un throughput di trasferimento da/verso la scheda pari a 16 GB/s
- dalla quantità di memoria esterna disponibile: 2 banchi di memoria DDR, ognuno di 16 GB, per una banda totale verso la memoria BW_{DDR}=38 GB/s ed un banco da 8 GB di memoria HBM con banda di memoria BW_{HBM}=460 GB/s (banda totale verso la memoria esterna BW = 0.5 TB/s)
- dalla disponibilità del flusso di progettazione Vitis, che include sia il flusso di progettazione basato su linguaggi descrittivi dell'hardware (VHDL, Verilog) che il flusso di progettazione basato sul linguaggio C/C++ (Vitis HLS).

È immediato riconoscere, nella scheda selezionata, la seguente gerarchia di memoria

Tipo di memoria	Dimensione	Banda di accesso	Latenza (cicli di clock)
Host	O(100) GB	16 GB/s	$O(10^3\text{-}10^4)$
Esterna (DDR/HBM)	40 GB	0.5 TB/s	$O(10^2)$
Interna (B-, Ultra-)RAM	37 MB	35 TB/s	1

La struttura della gerarchia di memoria dovrà essere tenuta ben presente quando si progetteranno gli algoritmi da implementare sulla scheda FPGA, avendo cura di strutturarli in modo da massimizzare la località esposta dagli accessi in memoria e minimizzando il traffico con i livelli più lenti della gerarchia.

Gli algoritmi di crittazione verranno sviluppati preferibilmente utilizzando il flusso di progettazione Vitis HLS (ver. 2023.1) che permette di esprimere gli algoritmi mediante programmi scritti in C/C++, arricchiti con direttiva "#pragma HLS …" per fornire indicazioni al compilatore, demandando poi al flusso di compilazione l'effettiva estrazione della concorrenza tra le varie operazioni e la massimizzazione del parallelismo (sia di calcolo che di trasferimento dati). Il flusso Vitis HLS permette di effettuare il debug dell'applicazione lavorando solamente a livello di C/C++, evitando i lunghi tempi di compilazione legati alla traduzione in HW del codice C/C++ (fase di verifica della correttezza funzionale); solo una volta che si è giunti ad un programma che sia funzionalmente corretto, il flusso Vitis HLS passa alla fase di traduzione in HW del codice C/C++ (corretta per costruzione): durante questa seconda fase vengono tenuti in considerazione gli aspetti legati alle prestazioni (effettiva estrazione del parallelismo, sovrapposizione delle operazioni di trasferimento dati con le fasi di calcolo, raggiungimento del throughput o, in generale, degli obiettivi prestazionale prefissati).

Per la protezione dei dati che transitano all'interno della VLAN, e della rete di campus in generale, si è scelto di adottare il firewall PA-3260 della Palo Alto Networks. Tale Firewall è stato progettato per gestire efficacemente il traffico derivato dalla Internet of Things (IoT): il firewall si interfaccia al servizio cloud IoT Security che impiega algoritmi di intelligenza artificiale e di apprendimento automatico per riconoscere, in maniera dinamica, i dispositivi IoT presenti nella rete. Tali dispositivi sono caratterizzati da pattern di traffico che tendono ad essere riconoscibili, in quanto generati da dispositivi che hanno un limitato set di funzionalità, a differenza delle reti di computer che sono in grado di effettuare una grande quantità di task e rendono quindi più difficile categorizzare le varie tipologie di traffico generate. Tramite gli algoritmi di AI, messi a

disposizione in ambiente cloud, il servizio IoT Security è in grado di riconoscere le tipologie di traffico lecite e di identificare tutti i dispositivi sulla rete. Il servizio, una volta creata una baseline che descrive il comportamento delle normali attività di rete, è in grado di monitorare continuamente la rete e identificare i comportamenti non usuali che possono rappresentare attacchi o violazione delle regole di sicurezza adottate, generando dei segnali di allerta da gestire opportunamente per garantire la continuità e la sicurezza del servizio.

Tra le funzionalità fornite dal firewall PA-3260, si trovano:

- la raccolta dei metadata derivati dal traffico sulla rete,
- la generazione di log da inviare al servizio IoT Security per l'analisi e la gestione delle eventuali minacce alla sicurezza,
- la gestione delle applicazioni tramite la loro funzionalità e non collegandole a classi di indirizzi fisici di porte/IP,
- la possibilità di abilitare/disabilitare la crittazione del traffico sulla base della categoria di URL, della zona in cui si trovano i soggetti della comunicazione, degli indirizzi IP, …

Per quanto riguarda il server di calcolo, che dovrà ospitare due schede FPGA Alveo U280, si è deciso di adottare dei sistemi SuperMicro, garantendo in questo modo l'omogeneità con gli altri sistemi già esistenti nel centro di calcolo. Si è scelto il server SuperMicro A+ Server 2024US-TRT che ha le seguenti caratteristiche:

- monta 2 processori AMD Milan 7313, ognuno equipaggiato con 16 core; ogni core ha 64KB di cache L1, 512KB di cache L2. Sono inoltre presenti 128 MB di cache L3 (condivisa tra tutti i core). La TDP del processore è 155W.
- offre 6 slot di espansione PCI-e Gen4 (x16 e x8)
- presenta 256 GB di memoria DDR4, suddivisa in 16 banchi, ognuno da 16 GB
- monta 2 SSD NVMe da 960 GB
- per la connettività usa 2 porte di rete10GBase-T integrate e 2 moduli transceiver SFP+ 10G ottici
- utilizza un alimentatore ridondante da 1600 W

Tale server, con i suoi 32 core (clock 3.7 GHz), slot PCIe Gen4x16, dischi NVMe e canali di connessione ottica garantisce le prestazioni di comunicazione e di calcolo sufficienti a:

- ricevere i dati generati dalla sensor VLAN,
- implementare le operazioni previste di crittazione tramite le schede FPGA Alveo U280 ospitate,
- gestire le operazioni di storage dei dati

Il sistema di storage sarà destinato ad ospitare il data base realizzato nella LA 3.9 e i vari log dei dati di traffico. Con l'obiettivo di omogeneizzarsi ai sistemi già presenti nel centro di calcolo di ENEA Casaccia, all'interno del quale verrà ospitata l'infrastruttura HPC che si sta realizzando, si è deciso di acquisire il seguente sistema SuperMicro SSG-6049P-E1CR24H che include

- 2 Processori Intel Xeon Bronze 3204, 6 core con clock a 1,9 GHz, TDP = 85W
- 96 GB di memoria DDR4, organizzati in 6 moduli di memoria da 16GB ECC Registered 2933 MHz
- Controller RAID, con 2 GB di cache dedicata,
    - SAS3 (12 Gb/s) livelli RAID 0,1, 5,6, 10, 50, 60
    - SATA (6 Gb/s) livelli RAID 0,1,5,10
- 2 SSD da 240 GB SATA per sistema operativo
- 24 Dischi rigidi 3.5" da 12 TB,7200 rpm,NL-SATA 6Gb/s inseriti nei 24 slot hot-swappable presenti
- Connettività LAN tramite 2 RJ45 10GBase-T LAN ports e 1 RJ45 Dedicated IPMI LAN port

La sicurezza derivante dalle configurazioni RAID, assieme alla tecnologia hot-swappable, garantisce l'affidabilità e la continuità del servizio richieste allo storage server.

Con lo scopo di testare la gestione di sensori/attuatori presenti nella VLAN e sviluppare le procedure di controllo senza interferire con i sensori che sono già in produzione nel Centro Ricerche Casaccia, si è deciso di acquisire alcuni sensori/attuatori, controllabili e interrogabili tramite la rete internet: tali sensori/attuatori, dotati ciascuno di un proprio indirizzo IP e controllabili tramite comandi http, verranno configurati all'interno della sensor VLAN.

In riferimento al sistema energetico, cui è principalmente destinata l'architettura HPC in fase di realizzazione, si è optato per acquisire degli smart meter gestiti da una scheda PLC, che presentano 4 prese controllabili da remoto e sono dotati di un proprio indirizzo IP; per ciascuna presa è possibile conoscere la tensione, la corrente erogata e la potenza assorbita dal carico collegato. Sono inoltre presenti due sensori di temperatura, anche questi interrogabili da remoto tramite richieste http.

I sensori saranno dislocati in palazzine differenti del C.R. Casaccia e saranno inseriti all'interno della stessa sensor VLAN.

Relativamente all'ambiente SW da adottare, si è optato per il seguente stack SW che prevede:

- OS Linux: la distribuzione da scegliere è ancora oggetto di studio, a seguito della chiusura del supporto alla distribuzione centOS
- Data base relazionale compatibile con SQL
- Il flusso di compilazione Vitis, con le relative librerie per la gestione del run-time, per le schede FPGA
- IoT security per il firewall

L'ambiente Linux, estremamente aperto, consentirà di aggiungere i vari pacchetti SW e librerie che si dovessero rendere necessari nel corso dello sviluppo del progetto.

Riportiamo in Figura 2 lo schema dell'infrastruttura di calcolo, definita in linea di principio in figura 1, specializzata evidenziando l'impiego dei dispositivi selezionati.

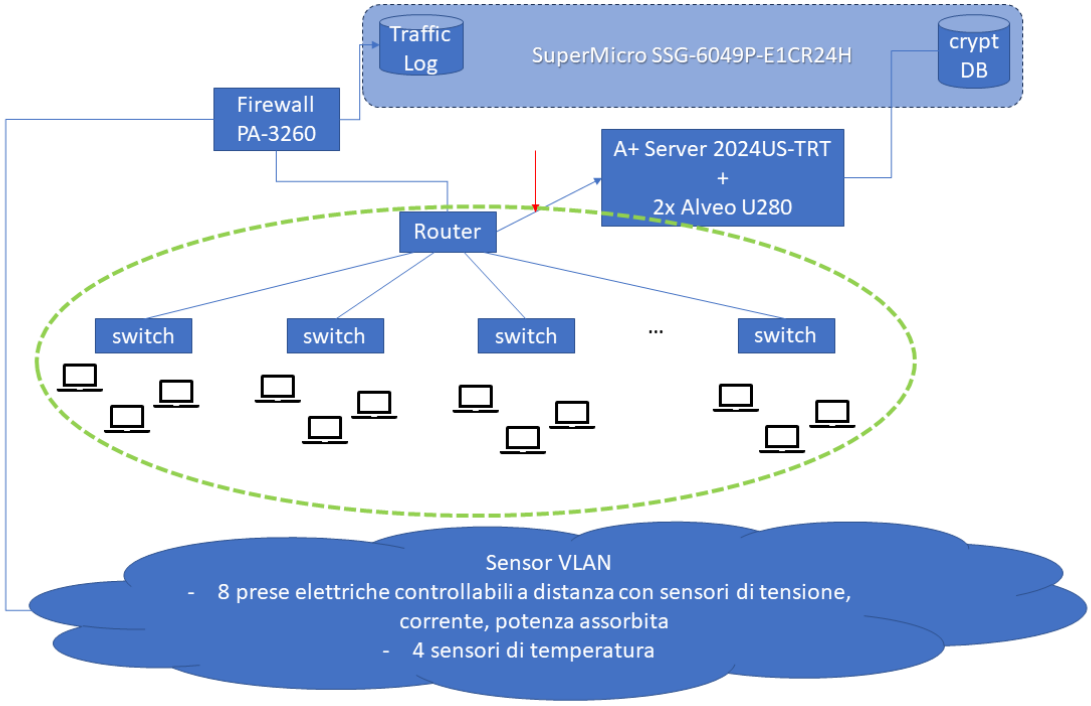

Fig. 2: schema finale dell' infrastruttura di calcolo HPC

8 Contributo delle eventuali consulenze alle attività sopra descritte

L'attività non ha previsto il ricorso a consulenze.

9 Pubblicazioni scientifiche

L'attività svolta non è stata oggetto di pubblicazioni scientifiche nel SAL.

10 Eventi di disseminazione

L'attività svolta non è stata oggetto di eventi di disseminazione specifici nel SAL.

11 Appendice A – Firewall

paloalto NETWORKS | STRATA

PA-3260

PA-3250

PA-3220

PA-3200 Series

Palo Alto Networks PA-3200 Series ML-Powered NGFWs—comprising the PA-3260, PA-3250, and PA-3220—target high-speed internet gateway deployments. PA-3200 Series appliances secure all traffic, including encrypted traffic, using dedicated processing and memory for networking, security, threat prevention, and management.

Highlights

- World's first ML-Powered NGFW
- Eleven-time Leader in the Gartner Magic Quadrant for Network Firewalls
- Leader in The Forrester Wave: Enterprise Firewalls, Q4 2022
- Highest Security Effectiveness score in the 2019 NSS Labs NGFW Test Report with 100% of evasions blocked
- Extends visibility and security to all devices, including unmanaged IoT devices, without the need to deploy additional sensors
- Supports high availability with active/active and active/passive modes
- Delivers predictable performance with security services
- Simplifies deployment of large numbers of firewalls with optional Zero Touch Provisioning (ZTP)
- Supports centralized administration with Panorama network security management
- Maximizes security investments and prevents business disruptions with AIOps

The controlling element of the PA-3200 Series is PAN-OS, the same software that runs all Palo Alto Networks Next-Generation Firewalls (NGFWs). PAN-OS natively classifies all traffic, inclusive of applications, threats, and content, and then ties that traffic to the user regardless of location or device type. The application, content, and user—in other words, the elements that run your business—then serve as the basis of your security policies, resulting in improved security posture and reduced incident response time.

Key Security and Connectivity Features

ML-Powered Next-Generation Firewall

- Embeds machine learning (ML) in the core of the firewall to provide inline signatureless attack prevention for file-based attacks while identifying and immediately stopping never-before-seen phishing attempts.
- Leverages cloud-based ML processes to push zero-delay signatures and instructions back to the NGFW.
- Uses behavioral analysis to detect internet of things (IoT) devices and make policy recommendations; cloud-delivered and natively integrated service on the NGFW.
- Automates policy recommendations that save time and reduce the chance of human error.

Identifies and Categorizes All Applications, on All Ports, All the Time, with Full Layer 7 Inspection

- Identifies the applications traversing your network irrespective of port, protocol, evasive techniques, or encryption (TLS/SSL).
- Automatically discovers and controls new applications to keep pace with the SaaS explosion with SaaS Security subscription.
- Uses the application, not the port, as the basis for all your safe enablement policy decisions: allow, deny, schedule, inspect, and apply traffic-shaping.
- Offers the ability to create custom App-ID tags for proprietary applications or request App-ID development for new applications from Palo Alto Networks.
- Identifies all payload data within the application (e.g., files and data patterns) to block malicious files and thwart data exfiltration attempts.
- Creates standard and customized application usage reports, including software-as-a-service (SaaS) reports that provide insight into all sanctioned and unsanctioned SaaS traffic on your network.
- Enables safe migration of legacy Layer 4 rule sets to App-ID-based rules with built-in Policy Optimizer, giving you a rule set that is more secure and easier to manage.

Enforces Security for Users at Any Location, on Any Device, While Adapting Policy Based on User Activity

- Enables visibility, security policies, reporting, and forensics based on users and groups—not just IP addresses.
- Easily integrates with a wide range of repositories to leverage user information: wireless LAN controllers, VPNs, directory servers, SIEMs, proxies, and more.
- Allows you to define Dynamic User Groups (DUGs) on the firewall to take time-bound security actions without waiting for changes to be applied to user directories.
- Applies consistent policies irrespective of users' locations (office, home, travel, etc.) and devices (iOS and Android mobile devices, macOS, Windows, Linux desktops, laptops; Citrix and Microsoft VDI and Terminal Servers).
- Prevents corporate credentials from leaking to third-party websites and prevents reuse of stolen credentials by enabling multifactor authentication (MFA) at the network layer for any application without any application changes.
- Provides dynamic security actions based on user behavior to restrict suspicious or malicious users.
- Consistently authenticates and authorizes your users, regardless of location and where user identity stores live, to move quickly toward a Zero Trust security posture with Cloud Identity Engine—an entirely new cloud-based architecture for identity-based security. Check out the Cloud Identity Engine solution brief for more information.

Prevents Malicious Activity Concealed in Encrypted Traffic

- Inspects and applies policy to TLS/SSL-encrypted traffic, both inbound and outbound, including for traffic that uses TLS 1.3 and HTTP/2.
- Offers rich visibility into TLS traffic, such as amount of encrypted traffic, TLS/SSL versions, cipher suites, and more, without decrypting.
- Enables control over use of legacy TLS protocols, insecure ciphers, and misconfigured certificates to mitigate risks.
- Facilitates easy deployment of decryption and lets you use built-in logs to troubleshoot issues, such as applications with pinned certificates.
- Lets you enable or disable decryption flexibly based on URL category, source and destination zone, address, user, user group, device, and port, for privacy and regulatory compliance purposes.
- Allows you to create a copy of decrypted traffic from the firewall (i.e., decryption mirroring) and send it to traffic collection tools for forensics, historical purposes, or data loss prevention (DLP).
- Allows you to intelligently forward all traffic (decrypted TLS, nondecrypted TLS, and non-TLS) to third-party security tools with Network Packet Broker, optimize your network performance, and reduce operating expenses.
- Refer to this decryption whitepaper to learn where, when, and how to decrypt to prevent threats and secure your business.

Offers Centralized Management and Visibility

- Benefits from centralized management, configuration, and visibility for multiple distributed Palo Alto Networks NGFWs (irrespective of location or scale) through Panorama network security management, in one unified user interface.
- Streamlines configuration sharing through Panorama with templates and device groups, and scales log collection as logging needs increase.
- Enables users, through the Application Command Center (ACC), to obtain deep visibility and comprehensive insights into network traffic and threats.

Maximize Your Security Investment and Prevent Business Disruption with AIOps

- AIOps for NGFW delivers continuous best practice recommendations customized to your unique deployment to strengthen your security posture and get the most out of your security investment.
- Intelligently predicts firewall health, performance, and capacity problems based on ML powered by advanced telemetry data. It also provides actionable insights to resolve the predicted disruptions.

Detects and Prevents Advanced Threats with Cloud-Delivered Security Services

Today's sophisticated cyberattacks can spawn 45,000 variants in 30 minutes using multiple threat vectors and advanced techniques to deliver malicious payloads. Traditional siloed security causes challenges for organizations by introducing security gaps, increasing overhead for security teams, and hindering business productivity with inconsistent access and visibility.

Seamlessly integrated with our industry-leading NGFWs, our Cloud-Delivered Security Services use the network effect of 80,000 customers to instantly coordinate intelligence and protect against all threats across all vectors. Eliminate coverage gaps across your locations and take advantage of best-in-class security delivered consistently in a platform to stay safe from even the most advanced and evasive threats. Services include:

- **Advanced Threat Prevention**: Stop known exploits, malware, spyware, and command-and-control (C2) threats while utilizing industry-first prevention of zero-day attacks—prevent 60% more unknown injection attacks and 48% more highly evasive command-and-control traffic than traditional IPS solutions.
- **Advanced WildFire**: Ensure files are safe by automatically preventing known, unknown, and highly evasive malware 60X faster with the industry's largest threat intelligence and malware prevention engine.
- **Advanced URL Filtering**: Ensure safe access to the internet and prevent 40% more web-based attacks with the industry's first real-time prevention of known and unknown threats, stopping 88% of malicious URLs at least 48 hours before other vendors.
- **DNS Security**: Gain 40% more threat coverage and stop 85% of malware that abuses DNS for command and control and data theft without requiring changes to your infrastructure.

- **Enterprise DLP**: Minimize risk of a data breach, stop out-of-policy data transfers, and enable compliance consistently across your enterprise with 2X greater coverage of any cloud-delivered enterprise DLP.
- **SaaS Security**: Stay ahead of the SaaS explosion with the industry's only Next-Generation CASB to automatically see and secure all apps across all protocols.
- **IoT Security**: Safeguard every "thing" and implement Zero Trust device security 20X faster with the industry's smartest security for smart devices.

Delivers a Unique Approach to Packet Processing with Single-Pass Architecture

- Performs networking, policy lookup, application and decoding, and signature matching—for all threats and content—in a single pass. This significantly reduces the amount of processing overhead required to perform multiple functions in one security device.
- Avoids introducing latency by scanning traffic for all signatures in a single pass, using stream-based, uniform signature matching.
- Enables consistent and predictable performance when security subscriptions are enabled. (In table 1, "Threat Prevention throughput" is measured with multiple subscriptions enabled.)

Enables SD-WAN Functionality

- Allows you to easily adopt SD-WAN by simply enabling it on your existing firewalls.
- Enables you to safely implement SD-WAN, which is natively integrated with our industry-leading security.
- Delivers an exceptional end-user experience by minimizing latency, jitter, and packet loss.

Table 1: PA-3200 Series Performance and Capacities

	PA-3220	PA-3250	PA-3260
Firewall throughput (HTTP/appmix)*	3.7/4.2 Gbps	4.6/5.0 Gbps	6.9/7.8 Gbps
Threat Prevention throughput (HTTP/appmix)†	1.9/2.3 Gbps	2.4/2.7 Gbps	3.6/4.3 Gbps
IPsec VPN throughput‡	2.4 Gbps	2.6 Gbps	4.4 Gbps
Max concurrent sessions§	1M	2M	2.2M
New sessions per second‖	46,000	58,000	84,000
Virtual systems (base/max)#	1/6	1/6	1/6

Note: Results were measured on PAN-OS 11.0.

* Firewall throughput is measured with App-ID and logging enabled, utilizing 64 KB HTTP/appmix transactions.
† Threat Prevention throughput is measured with App-ID, IPS, antivirus, antispyware, WildFire, DNS Security, file blocking, and logging enabled, utilizing 64 KB HTTP/appmix transactions.
‡ IPsec VPN throughput is measured with 64 KB HTTP transactions and logging enabled.
§ Max concurrent sessions are measured utilizing HTTP transactions.
‖ New sessions per second is measured with application override, utilizing 1 byte HTTP transactions.
Adding virtual systems over base quantity requires a separately purchased license.

Table 2: PA-3200 Series Networking Features

Interface Modes
L2, L3, tap, virtual wire (transparent mode)
Routing
OSPFv2/v3 with graceful restart, BGP with graceful restart, RIP, static routing
Policy-based forwarding
Point-to-Point Protocol over Ethernet (PPPoE)
Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3
SD-WAN
Path quality measurement (jitter, packet loss, latency)
Initial path selection (PBF)
Dynamic path change
IPv6
L2, L3, tap, virtual wire (transparent mode)
Features: App-ID, User-ID, Content-ID, WildFire, and SSL decryption
SLAAC

Table 2: PA-3200 Series Networking Features (continued)
IPsec and SSL VPN
Key exchange: manual key, IKEv1, and IKEv2 (pre-shared key, certificate-based authentication)
Encryption: 3des, AES (128-bit, 192-bit, 256-bit)
Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512
GlobalProtect Large Scale VPN for simplified configuration and management*
Secure access over IPsec and SSL VPN tunnels using GlobalProtect gateway and portals*
VLANs
802.1Q VLAN tags per device/per interface: 4,094/4,094
Aggregate interfaces (802.3ad), LACP
Network Address Translation
NAT modes (IPv4): static IP, Dynamic IP, Dynamic IP and Port (port address translation)
NAT64, NPTv6
Additional NAT features: Dynamic IP reservation, tunable Dynamic IP and Port oversubscription
High Availability
Modes: active/active, active/passive, HA clustering
Failure detection: path monitoring, interface monitoring
Zero Touch Provisioning (ZTP)
Available with -ZTP SKUs (PA-3260-ZTP, PA-3250-ZTP, PA-3220-ZTP). Requires Panorama 9.1.3 or higher

* Requires GlobalProtect license.

Table 3: PA-3200 Series Hardware Specifications
I/O
PA-3220: 10/100/1000 (12), 1G SFP (4), 1G/10G SFP/SFP+ (4)
PA-3250: 10/100/1000 (12), 1G/10G SFP/SFP+ (8)
PA-3260: 10/100/1000 (12), 1G/10G SFP/SFP+ (8), 40G QSFP+ (4)
Management I/O
10/100/1000 out-of-band management port (1), 10/100/1000 high availability (2), 10G SFP+ high availability (1), RJ-45 console port (1), Micro USB (1)
Storage Capacity
240 GB SSD
Power Supply (Avg/Max Power Consumption)
Redundant 650-watt AC or DC (195/240)
Max BTU/hr
819
Input Voltage (Input Frequency)
AC: 100–240 VAC (50–60Hz)
DC: -48V to -60V
Max Current Consumption
AC: 2.3 A @ 100 VAC, 1.0 A @ 240 VAC
DC: -48 V @ 4.7 A, -60 V @ 3.8 A
Mean Time Between Failure (MTBF)
14 years
Rack Mount Dimensions
2U, 19" standard rack (3.5" H x 20.53" D x 17.34" W)

Table 3: PA-3200 Series Hardware Specifications (continued)
Weight (Standalone Device/As Shipped)
29 lbs / 41.5 lbs
Safety
cTUVus, CB
EMI
FCC Class A, CE Class A, VCCI Class A
Certifications
See paloaltonetworks.com/company/certifications.html
Environment
Operating temperature: 32°F to 122°F, 0°C to 50°C
Nonoperating temperature: -4°F to 158°F, -20°C to 70°C
Humidity tolerance: 10% to 90%
Maximum altitude: 10,000 ft / 3,048 m
Airflow: front to back

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

12 Appendice B – Computing servers

SUPERMICRO | AMD

DATASHEET

H12 Ultra Servers

Industry-Leading IOPS, Energy Efficiency, and Flexibility

1U A+ Server 1024US-TRT (SATA)

1U A+ Server 1124US-TNRP (NVMe)

2U A+ Server 2024US-TRT (SATA)

2U A+ Server 2124US-TNRP (NVMe)

Enterprise-focused platform designed for utmost performance and flexibility

Gain high performance, flexibility, scalability and serviceability to demanding IT environments, and to power mission-critical enterprise workloads:

- Two 2nd or 3rd Gen AMD EPYC™ processors
- Up to 32 DIMMs for up to 8 TB of DDR4-3200 memory
- Flexible NVMe and SATA3 drive options
- Dual 10 Gigabit Ethernet connectivity
- Titanium-Level efficiency power supplies

The biggest enemy of datacenter productivity is complexity. The more you have one-off servers performing unique functions, the more you have to maintain different firmware revisions, BIOS settings, and operating system patches where configuration errors or oversights can imperil application availability and even security. What you need is a base platform that can deliver all the performance you need but with with a consistent foundation that can support all of your applications.

Introducing H12 Ultra Servers

We designed H12 Ultra servers to be your flagship datacenter systems, certified to run the major enterprise applications. The product line is built to deliver a flexible range of computing, networking, storage, and expansion capacities, with options for hard-disk and NVMe drives offering a range of I/O operations per second (IOPS). Every one of our Ultra servers is based on the same H12DSU-iN motherboard with two AMD EPYC™ processors and 32 DDR-3200 DIMMs for up to 8 TB of main memory. Consistency means you have only one set of firmware, BIOS settings, and operating system patches to manage. Every system built on this motherboard is designed for reliability, availability and serviceability so that if a problem occurs, your applications can be back up and running quickly.

Best of all, every H12 Ultra server is engineered to accommodate every processor in the 3rd Gen AMD EPYC processor product line, including those consuming up to 280W per CPU. AMD EPYC processors, with up to 64 cores of computing power and up to 768 MB of L3 cache per CPU, deliver the fastest integer and floating point performance in the industry, predicting ultra-fast performance for your enterprise applications. With a consistent set of features across the product line, you choose the number of cores your workloads need without having to step up the product line to gain additional features. The CPU's 128 lanes of PCI-E 4.0 bandwidth enables direct connectivity between the CPU and the newest U.2 NVMe drives with no intervening switching for extremely low storage latency.

AMD EPYC

Designed for Enterprise Applications

You want ultra performance for your enterprise applications, and the flexible selection of density and storage capacity gives you a server for every purpose, including:

- Enterprise applications including database, customer relationship management, and enterprise resource planning
- Virtualization and cloud, including virtual desktop infrastructure with GPU acceleration
- Hyperconverged infrastructure
- High performance computing clusters

Flexible Storage Configurations

As the tables below indicate, the four servers enjoy common features from the H12DSU-iN motherboard, and depending on their form factor and storage configuration, they offer varying sizes and types of storage:

- The AS -1024US-TRT and AS -2024US-TRT servers support 4 and 12 3.5" SAS or SATA drives (respectively) for the maximum amount of storage capacity, supporting hyperconverged infrastructure, enterprise databases, streaming, and big data applications.
- The AS -1124US-TNRP and AS -2124US-TNRP servers support the new U.2 NVMe drives with 12 in the 1U server and up to 24 in the 2U server, supporting mission-critical enterprise and low-latency financial applications; virtualized, cloud, and hyperconverged environments. Additional 10 Gigabit Ethernet SFP+ ports supports data-intensive clusters.

Consistent Management

You can manage all of your Ultra servers from a single pane of glass with Supermicro® SuperCloud Composer with open-source Redfish® compatibility.

H12 Generation	Common H12DSU-iN Motherboard Features
Processor Support	• Single SP3 socket for one AMD EPYC™ 7002 or 7003 Series processor including those with AMD 3D V-Cache™ technology • Up to 64 cores, up to 280W TDP*
Memory Slots & Capacity	• 32 DIMM slots for DDR4-3200 MHz RDIMM/LRDIMM • Up to 8 TB registered ECC
On-Board Devices	• System on Chip • IMPI 2.0 with virtual-media-over-LAN and KVM-over-LAN support • ASPEED AST2500 BMC graphics
I/O Ports	• Integrated IPMI 2.0 + KVM with dedicated LAN • 3 USB 3.0 ports (2 rear plus 1 Type A) • 1 VGA, 1 COM port • 1 TPM 2.0 header
BIOS and BIOS features	• AMI 128Mb SPI Flash EEPROM • Plug and Play (PnP) • DMI 2.3 • PCI 2.2 • ACPI 5.1 • USB Keyboard Support • SMBIOS 3.1.1
Front Panel	• Power On/Off and System Reset buttons • Power status, HDD activity, network activity, system overheat, fan failure, and UID LEDs
System Management	• Integrated IPMI 2.0 plus KVM with dedicated LAN • Redfish APIs • Supermicro SuperCloud Composer

*Certain CPUs with high TDP may be supported only under specific conditions. Please contact Supermicro Technical Support for additional information about specialized system optimization.

1U Servers	Dual-Socket AS -1024US-TRT	Dual-Socket AS -1124US-TNRP
Form Factor	• 1U rackmount	• 1U rackmount
Drive Bays	• 4 hot-swap 3.5" SATA3 drives or 4 NVMe (via optional drive tray) or 4 SAS3 (via optional SAS kit)	• 12 Hot-swap 2.5" U.2 NVMe drives or 12 SATA3/SAS3 (via optional SAS kit)
Expansion Slots	• 2 PCI-E 4.0 x16 (FH/9.5"L) slots • 1 PCI-E 4.0 x16 (LP) slot • 1 PCI-E 4.0 x16 (internal proprietary LP slot)	• 2 PCI-E 4.0 x16 (FH/9.5"L) slots • 1 PCI-E 4.0 x16 (LP) slot • 1 PCI-E 4.0 x16 (internal proprietary LP slot)
Networking	• Dual 10GBase-T LAN ports	• Dual 10GBase-T and 10G SFP+ ports
Power & Cooling	• 1000W Redundant Power Supplies (Titanium Level)	• 1200W Redundant Power Supplies (Titanium Level)

2U Servers	Dual-Socket AS -2024US-TRT	Dual Socket AS -2124US-TNRP
Form Factor	• 2U rackmount,	• 2U rackmount
Drive Bays	• 12 hot-swap 3.5" SATA 3 drives or 8 SATA3 + 4 NVMe via optional tray or 12 SAS3 via optional SAS kit	• 24 hot-swap 2.5" U.2 NVMe drives or or up to 24 SATA/SAS drive support via optional SAS kit
Expansion Slots	• 2 PCI-E 4.0 x16 (FH, 10.5"L) slots, • 1 PCI-E 4.0 x16 (FH, 9.5"L) slot, • 1 PCI-E 4.0 x16 (LP) slot, • 1 PCI-E 4.0 x8 (FH, 9.5"L, in x16) slot, • 1 PCI-E 4.0 x8 (internal proprietary LP in x16) slot	• 1 PCI-E 4.0 x16 slot (FH, 9.5"L)
Networking	• Dual 10GBase-T LAN ports	• Dual 10GBase-T and 10G SFP+ ports
Power & Cooling	• 1600W Redundant Power Supplies (Titanium Level)	• 1600W Redundant Power Supplies (Titanium Level)

SUPERMICRO

13 Appendice C – Storage node

1.3 System Features

The following table provides you with an overview of the main features of the SSG-6049P-E1CR24H/L. Please refer to Appendix C for additional specifications.

System Features
Motherboard
X11DPH-T
Chassis
SC846BE1C-R1K23B
CPU
Dual Intel Xeon 81xx/61xx/51xx/41xx/31xx series or 82xx/62xx/52xx/42xx/32xx series processors*
Socket Type
Socket P
Memory
16 DIMM slots support up to 4TB of Registered DIMM (RDIMM) or 3DS LRDIMM DDR4-2933 ECC memory (supports up to four Intel Optane DCPMMs)
Chipset
Intel C622 chipset
Expansion Slots
Four PCI-Express 3.0 x8 slots supported by CPU1 (Slots 1, 3, 6, 7) Three PCI-Express 3.0 x16 slots supported by CPU2 (Slots 2, 4, 5)
Hard Drives
24 hot-swap 3.5" hard drives
Power
1200W power supply (PWS-1K23A-1R)
Form Factor
4U rackmount
Dimensions
(WxHxD) 17.2 x 7 x 26.5 in. (437 x 178 x 673 mm)

***Note:** This server will support a Fabric processor in the CPU1 socket. FPGA processors are not supported.

1.4 Server Chassis Features

Control Panel

The switches and LEDs located on the control panel are described below. See Chapter 4 for details on the control panel connections.

Figure 1-1. Control Panel View

Control Panel Features		
Item	**Feature**	**Description**
1	Power Button	The power button is used to apply or remove power to the server. Turning off system power with this button removes the main power but maintains standby power. To perform many maintenance tasks, you must also unplug system before servicing
2	Reset Button	Used to reboot the system.
3	Power LED	Indicates power is being supplied to the system power supply. This LED should normally be illuminated when the system is operating.
4	HDD LED	Indicates activity on a hard drive when flashing.
5	NIC1	Indicates network activity on LAN port 1 when flashing
6	NIC2	Indicates network activity on LAN port 2 when flashing
7	System Overheat LED	Indicates an overheating condition in the system
8	Power Fail LED	Indicates a power supply module has failed

Front Features

The SC846BE1C-R1K23B is a 4U chassis See the illustration below for the features included on the front of the chassis.

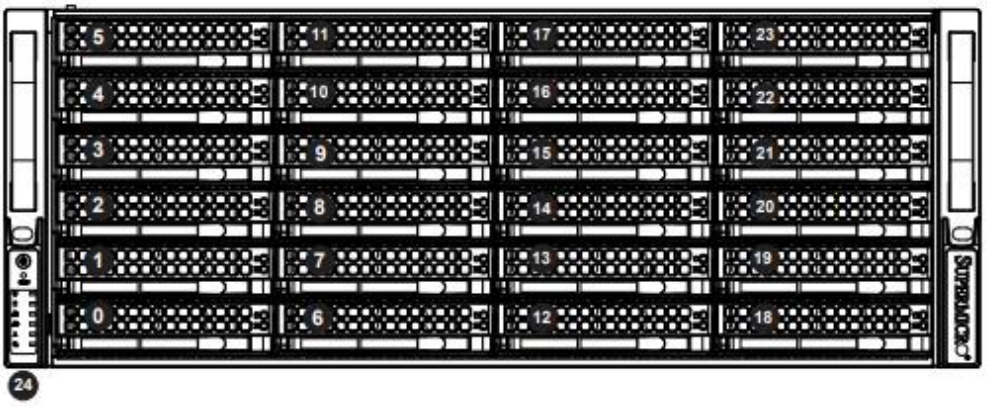

Figure 1-2. Chassis Front View

Front Chassis Features		
Item	**Feature**	**Description**
0-23	Hard Drive Carrie	Logical drive bay number for hot-swap hard drives
24	Control Panel	Control panel (see previous page for details)

Rear Features

The illustration below shows the features included on the rear of the chassis.

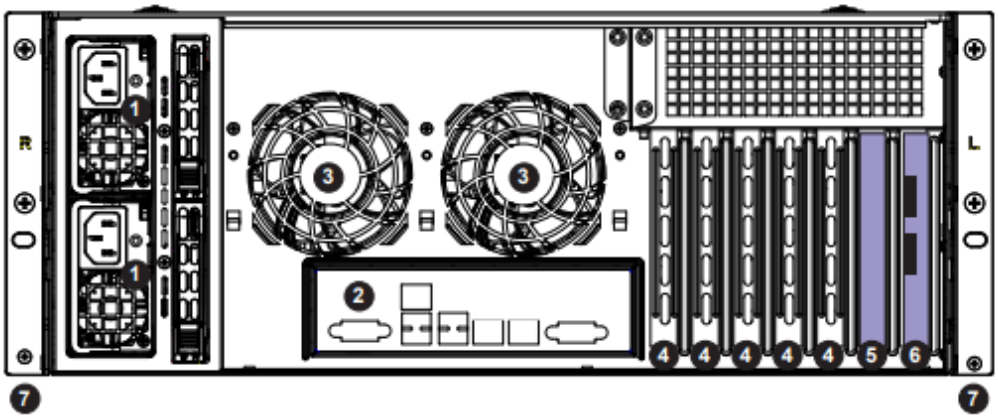

Figure 1-3. Chassis Rear View

Rear Chassis Features		
Item	**Feature**	**Description**
1	Power Supply Module	1200W power supply (redundant, with two power modules)
2	I/O Ports	I/O ports (see Section 4.3 for details)
3	Fan	8-cm rear exhaust fan
4	PCI Slots	Seven low-profile PCI slots for add-on cards
5	Add-on Card	Hardware RAID add-on card
6	Add-on Card	JBOD expansion card
7	Rack Ear Brackets	Attaches server chassis to the rack

1.5 Motherboard Layout

Below is a layout of the X11DPH-T with jumper, connector and LED locations shown. See the table on the following page for descriptions. For detailed descriptions, pinout information and jumper settings, refer to Chapter 4.

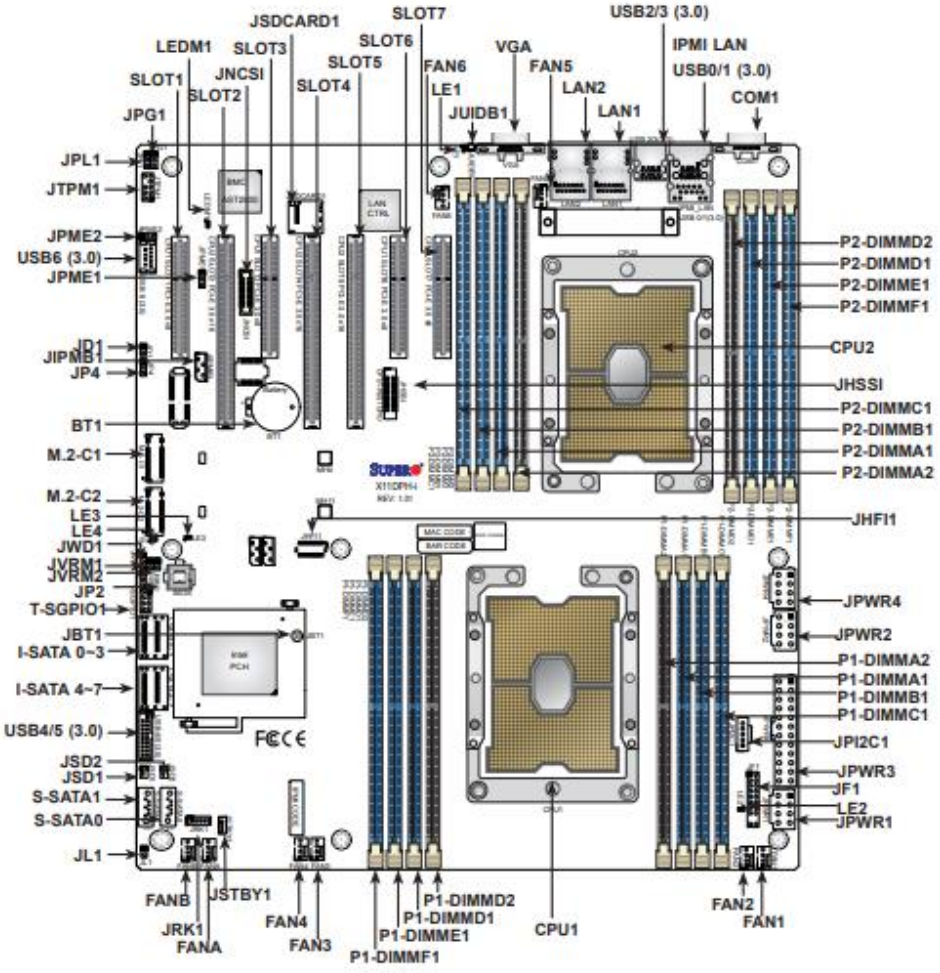

Figure 1-4. Motherboard Layout

Notes:

- Components not documented are for internal testing only.
- "▪" indicates the location of pin 1.

Quick Reference Table

Jumper	Description	Default Setting
JBT1	CMOS Clear	Open (Normal)
JPG1	VGA Enable	Pins 1-2 (Enabled)
JPL1	LAN1/LAN2 Enable	Pins 1-2 (Enabled)
JPME1	ME Recovery	Pins 1-2 (Normal)
JPME2	ME Manufacturing Mode	Pins 1-2 (Normal)
JVRM1	VRM SMB Clock (to BMC or PCH)	Closed (Normal: SMB Clock to BMC)
JVRM2	VRM SMB Data (to BMC or PCH)	Closed (Normal: SMB Clock to BMC)
JWD1	Watch Dog Timer Enable	Pins 1-2 (Reset)

Connector	Description
BT1	Onboard CMOS battery
COM1	COM port
FAN1~6, FANA/FANB	System/cooling fan headers
IPMI_LAN	Dedicated IPMI LAN port
I-SATA0~3, I-SATA4~7	SATA 3.0 Ports supported by the Intel PCH
JD1	Speaker header
JF1	Front control panel header
JHFI1	Host Fabric Interface (HFI) sideband connection header used for HFI carrier card
JHSSI	High-Speed Serial Interface (HSSI) card header
JIPMB1	4-pin external I²C Header (for an IPMI card)
JL1	Chassis intrusion header
JNCSI	Network Controller Sideband Interface (NCSI) header
JPI²C1	Power I²C System Management Bus (SMBus) header
JPWR1, JPWR2, JPWR4	8-pin power supply connectors
JPWR3	24-pin ATX main power supply connector
JRK1	Intel RAID key for NVMe SDD
JSD1, JSD2	SATA DOM (Device-on-Module) power connectors
JSDCARD1	Micro SD card slot
JSTBY1	Standby power header
JTPM1	Trusted Platform Module (TPM)/Port 80 connector
JUIDB1	Unit Identifier (UID) switch
LAN1, LAN2	10GbE LAN ports
M.2-C1, M.2-C2	M.2 slots
MH4, MH11	M.2 mounting holes
(CPU1) SLOT1, SLOT3, SLOT6, SLOT7	PCI-Express 3.0 x8 slots supported by CPU1

Connector	Description
(CPU2) SLOT2, SLOT4, SLOT5	PCI-Express 3.0 x16 slot supported by CPU2
S-SATA0, S-SATA1	Powered SATA 3.0 ports with support of Supermicro SuperDOM (Disk-On-Module)
T-SGPIO1	Serial Link General Purpose I/O (SGPIO) port
USB0/1, USB2/3	Universal Serial Bus (USB) 3.0 ports
USB4/5	Internal USB 3.0 header for front access
USB6	Type A USB 3.0 header for front access
VGA	VGA port

LED	Description	Status
LE1	Unit Identifier (UID) LED	Solid Blue: Unit Identified
LE2	Onboard power LED	Solid Green: Power On
LEDM1	BMC Heartbeat LED	Blinking Green: BMC normal

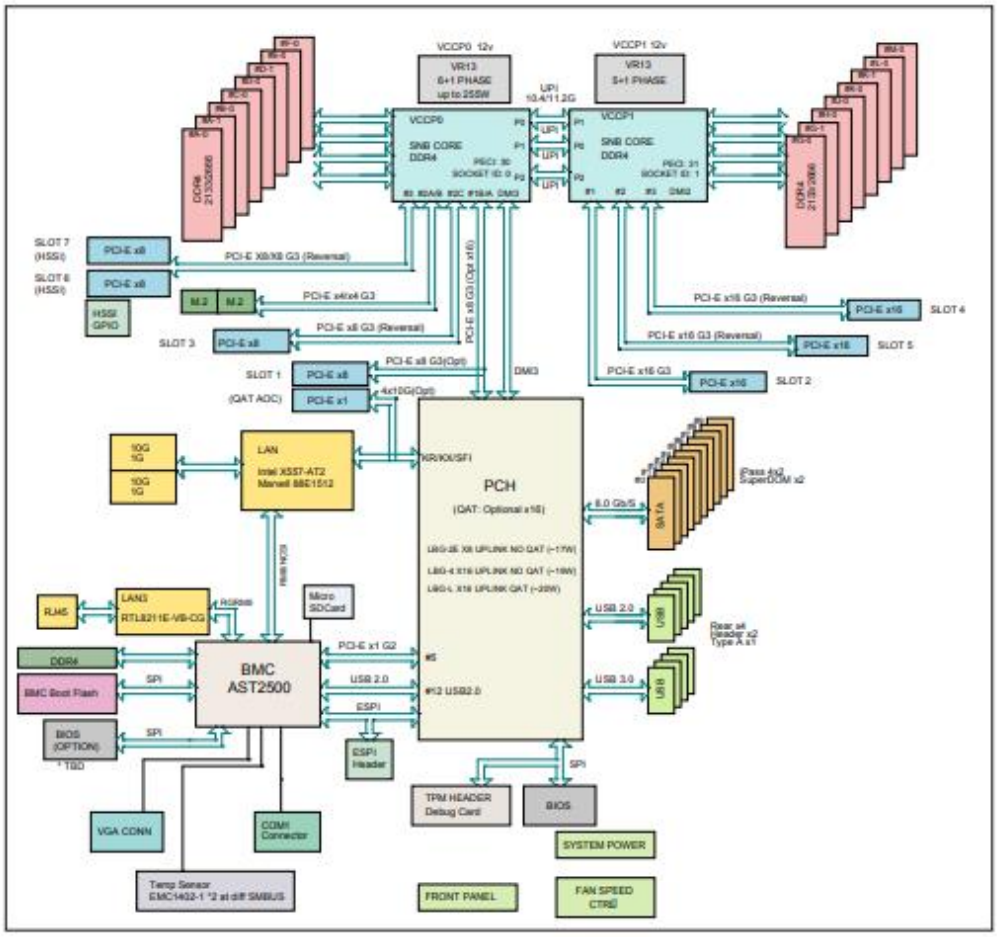

Figure 1-5. Intel C622 Chipset: System Block Diagram

Note: This is a general block diagram and may not exactly represent the features on your motherboard. See the System Specifications appendix for the actual specifications of your motherboard.

Appendix C

System Specifications

Processors	
Dual Intel Xeon 81xx/61xx/51xx/41xx/31xx series or 82xx/62xx/52xx/42xx/32xx series processors in a Socket P type socket **Note:** Please refer to the motherboard specifications pages on our website for updates to supported processors.	
Chipset	
Intel C622 chipset	
BIOS	
256 Mb AMI® Flash ROM	
Memory	
16 DIMM slots support up to 4TB of Registered DIMM (RDIMM) or 3DS LRDIMM DDR4-2933 ECC memory (supports up to four Intel Optane DCPMMs) **Note:** 2933 MHz memory is supported by the 82xx/62xx/52xx platform only. Only Platinum-level and Gold-level processors support Intel OptaneTM DC Persistent Memory Module (DCPMM).See the memory section in Chapter 3 for details and our website for updates to supported memory.	
SATA Controller	
Intel C622 controller	
Drive Bays	
Supports up to 24 hot-swap 3.5" hard drives	
PCI Expansion Slots	
Four PCI-Express 3.0 x8 slots supported by CPU1 (Slots 1, 3, 6, 7) Three PCI-Express 3.0 x16 slots supported by CPU2 (Slots 2, 4, 5)	
Motherboard	
X11DPH-T; ATX form factor (W x L) 13" x 12" (330 mm x 305 mm)	
Chassis	
SC846BE1C-R1K23B; 4U Rackmount, (WxHxD) 17.2 x 7 x 26.5 in. (437 x 178 x 673 mm)	
System Cooling	
Three 8-cm cooling fans and two 8-cm exhaust fans	
Power Supply	
Redundant 1200W power supply modules AC Input Voltages: 100-240 VAC Rated Input Current: 100-127V: 15-12A, 200-240V: 8.5-7A Rated Input Frequency: 50-60 Hz Rated Output Power: 1200W Rated Output Voltages: +12V (83A max. for 100-127A, 100A max. for 200-240A), +5Vsb (4A max.)	
Operating Environment	
Operating Temperature: 10° to 35° C (50° to 95° F) Non-operating Temperature: -40° to 60° C (-40° to 140° F) Operating Relative Humidity: 8% to 90% (non-condensing) Non-operating Relative Humidity: 5% to 95% (non-condensing)	

Regulatory Compliance

Electromagnetic Emissions: FCC Class A, EN 55032 Class A, EN 61000-3-2/3-3, CISPR 22 Class A
Electromagnetic Immunity: EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11)
Safety: CSA/EN/IEC/UL 60950-1 Compliant, UL or CSA Listed (USA and Canada), CE Marking (Europe)
Other: VCCI-CISPR 32 and AS/NZS CISPR 32
Environmental: Directive 2011/65/EU, Delegated Directive (EU) 2015/863 and Directive 2012/19/EU

Perchlorate Warning

California Best Management Practices Regulations for Perchlorate Materials: This Perchlorate warning applies only to products containing CR (Manganese Dioxide) Lithium coin cells. "Perchlorate Material-special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate"