Tường lửa thế hệ mới Palo Alto

Tính năng và chi tiết kĩ thuật

VietSunshine Electronic Solution Join Stock Company

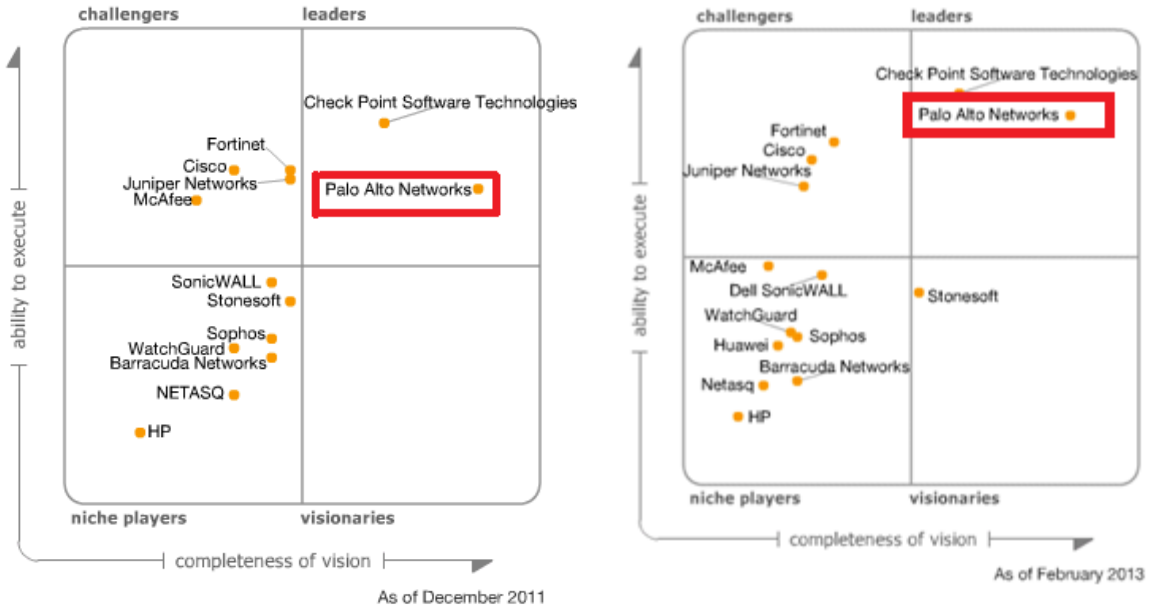
Central Garden, 225 Ben Chuong Duong St, Dist 1, HCMC VN

Phone: 84.8.3920 8030 | Fax: 84.8.3920 8040About Palo Alto Networks

1.1 Về công ty:

Palo Alto Networks là công ty về an ninh mạng. Là người có tầm nhìn về bảo mật và an ninh mạng, Nir Zuk sáng lập công ty vào năm 2005 định nghĩa lại về khái niệm an ninh mạng cho doanh nghiệp, bắt đầu với firewall. An ninh mạng trong hầu hết các doanh nghiệp là mảng bị phân mảnh và chia nhỏ, gây ra nhiều nguy cơ cho hoạt động kinh doanh của doanh nghiệp cũng như tăng chi phí.

Palo Alto Networks tin rằng firewall cần phải trở thành thiết bị an ninh quan trọng mang tính chiến lược trong một doanh nghiệp. Đội ngũ quản lý và ban giám đốc là những người đóng vai trò quan trọng trong lĩnh vực an ninh mạng hay những lĩnh vực liên quan bao gồm: phát minh công nghệ stateful inspection, hardware-based security, và ngăn ngừa xâm nhập (intrusion prevetion). Đội ngũ kỹ sư cuar Palo Alto giàu kinh nghiệm trong việc nghiên cứu các giải pháp an ninh như Checkpoint, Cisco, Netscreen, McAfee, Juniper Networks..v.v



Trong vòng 1 năm, thị phần của PAN đã tăng một cách nhanh chóng

Chúng tôi bắt đầu đưa ra thị trường sản phẩm firewall thế hệ mới năm 2007, và đến bây giờ đã triển khai giả pháp này cho trên 4500 khách hàng doanh nghiệp khắp thế giới, bao gồm 500 công ty lớn nhất theo Fortune. Vào tháng 8 năm 2011, Palo Alto Networks vượt ngưỡng 200 triệu đô la Mỹ, và vẫn tiếp tục tăng trưởng trong 5 quý vừa qua. Gartner đánh giá Palo Alto Networks là công ty có tầm nhìn về mặt công nghệ nhất trong thị trương firewall cho doanh nghiệp.

Tưởng lửa thế hệ mới Palo Alto

- **Nhận dạng, kiểm soát các ứng dụng:**

PAN cung cấp khả năng hiển thị và kiểm soát hệ thống thông qua các ứng dụng, người dùng và nội dung bất kể Port, giao thức, các phương thức lẩn tránh hoặc mã hoá

- **Kiểm soát nội dung của các đối tượng theo thời gian thực**

Cho phép người dùng thiết lập cơ chế quét và kiểm soát nội dung bên trong của các ứng dụng được gửi đi theo thời gian thực, để phát hiện các lỗ hổng bảo mật, virus, spyware, các dữ liễu nhạy cảm…

- **Thông lượng và hiệu suất làm việc cao**

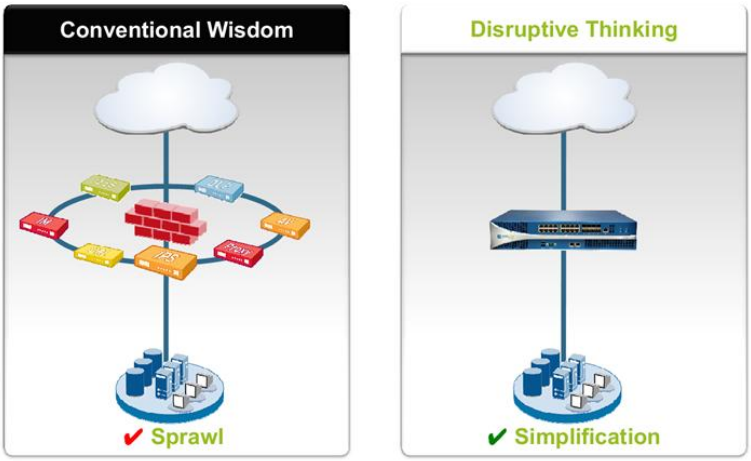
Với cơ chế quét thông minh và cấu trúc phần cứng được tối ưu hoá, hiệu suất làm việc của PAN luôn đảm bảo đáp ứng yêu cầu về tốc độ cho hệ thống.

- **Đơn giản hoá hệ thống bảo mật, giảm chi phí một cách hiệu quả.**

PAN cung cấp cho khách hàng một loạt các chức năng bảo mật quan trọng cần thiết từ Firewall, DLP, Anti-virus, IPS, URL Filtering…. trên một Box cứng duy nhất, tránh việc phải sử dụng quá nhiều thiết bị đơn lẻ trong hệ thống.

- **Môi trường hoạt động đa dạng.**

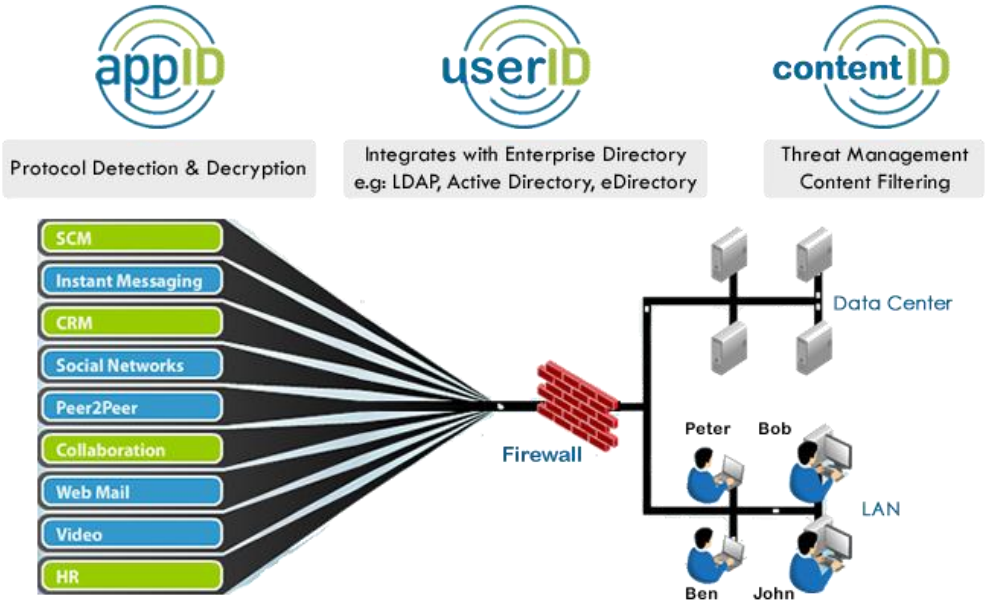
PAN có thể triển khai trên môi trường mạng doanh nghiệp, bao gồm cả các trung tâm dữ liệu, tại vành đai mạng, tại các chi nhánh , và trong các môi trường phát triển của điện toán đám mây, ảo hóa, và di động.



Hệ thống sẽ trở nên vô cùng đơn giản, quản lý dễ dàng, hoạt động hiệu quả với PA

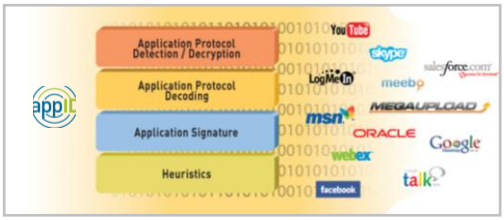
2 Công nghệ chính của Palo Alto Networks

Với kiến trúc phần cứng được thiết kế riêng biệt, firewall thế hệ mới Palo Alto mang lại sự tường minh và khả năng kiểm soát ứng dụng, người dùng, và nội dung sử dụng 3 công nghệ nhận dạng tiên tiến: App-ID, User-ID and Content-ID.

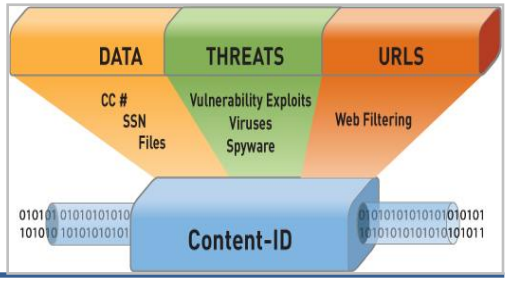


Ứng dụng tất cả công nghệ tiên tiến vào trong sản phẩm

App-ID: App-ID: sử dụng 4 cơ chế phân loại dữ liệu khác nhau, App-ID™ nhận dạng chính xác các ứng dụng nào thực sự đang chạy trên hạ tầng mạng mà không phụ thuộc vào ứng dụng đó đang chạy trên cổng dịch vụ gì, giao thức nào, hay đã được mã hóa SSL hay không. Nhờ đó giúp người quản trị có thể tạo những chính sách toàn diện để quản lí việc sử dụng ứng dụng và traffic inbound và outbound để gia tăng sự bảo mật của hệ thống hạ tầng mạng.

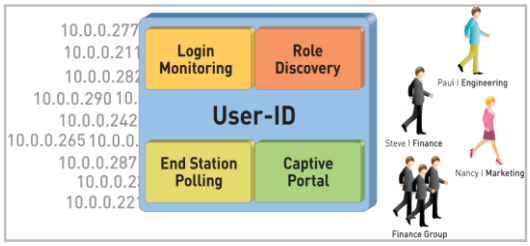


Content-ID: một engine quét dựa trên luồng dữ liệu (stream-based engine) giúp phát hiện và chặn các mối hiểm họa và giới hạn việc chuyển một cách trái phép các tập tin dữ liệu, nội dung nhạy cảm. Ngoài ra, cơ sở dữ liệu URL toàn diện kiểm soát việc lướt web không phục vụ cho công việc của nhân viên. Khả năng nhìn rõ và kiểm soát ứng dụng, cùng với khả năng ngăn ngừa các mối đe dọa nhờ vào Content-ID



cho phép phòng IT lấy lại khả năng kiểm soát ứng dụng và các mối đe dọa.

User-ID: Tích hợp với Microsoft Active Directory kết nối địa chỉ IP với người dùng, nhóm cho phép phòng IT kiểm soát ứng dụng, nội dung dựa trên thong tin nhân viên được lưu trong Active Directory. User-ID cho phép nhà quản trị kết hợp thông tin người dùng với ứng dụng, tạo policy, log dữ liệu và báo cáo.

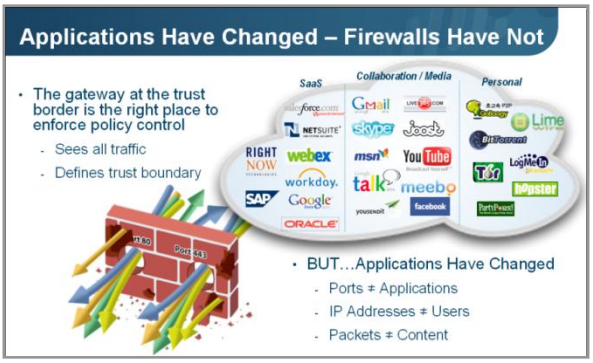


3 Mô tả giải pháp

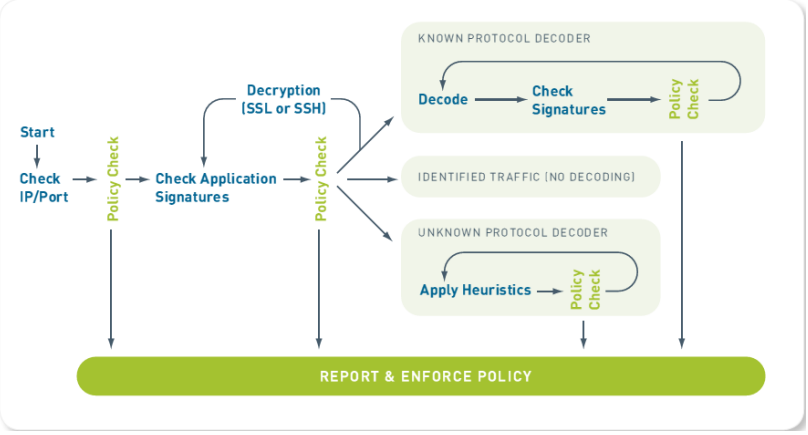
Sự phát triển của ứng dụng là thách thức đối với firewall ngày nay để bảo vệ mạng doanh nghiệp. Số lượng khách hàng và ứng dụng trong doanh nghiệp sử dụng các kỹ thuật lẩn tránh tinh vi như sử dụng port động hay ngẫu nhiên, giả dạng ứng dụng hay tạo đường hầm. Kết quả là mạng doanh nghiệp tràn ngập các ứng dụng không kiểm được soát được, vì firewall không nhìn thấy được. Điều này làm cho hệ thống mạng doanh nghiệp gặp phải các nguy cơ về an toàn cũng như vấn đề về tuân thủ các quy định. Để giải quyết sự mù mờ và khả năng kiểm soát ứng dụng, các doanh nghiệp cần một số công cụ

3.1 Nhận dạng và kiểm soát ứng dụng

Với sự phát triển vượt bật của ứng dụng Web ngày nay, port hay protocol không còn là dấu hiệu đặc trưng để nhận biết một ứng dụng. Ví dụ: các ứng dụng gmail, google doc, bittorrent, google talk tất cả đều chạy trên port 80… Vì vậy, các firewall truyền thống hoạt động dựa trên cơ chế stateful inspection không thể mang lại cho nhà quản trị cái nhìn toàn diện hệ thống mạng cũng như khả năng kiểm soát ứng dụng nữa.



Kỹ thuật nhận dạng ứng dụng là nền tảng của firewall thế hệ mới Palo Alto, được thực hiện trong một quy trình duy nhất, với 4 cơ chế phân loại dữ liệu khác nhau: Application Signature, Protocol Decoder, SSL decryption, Heuristics. Với cơ chế nhận dạng tiên tiến này cho phép phát hiện các ứng dụng lẩn tránh (evasive application) (ứng dụng nhảy port Skype) hay ứng dụng Proxy Ultrasurf cùng với những mối đe dọa mà nó mang lại cho hạ tầng mạng như thất thoát dữ liệu, malware, spyware…



3.2 Ngăn chặn hiểm họa theo thời gian thực

Khả năng nhận dạng và kiểm soát ứng dụng bằng App-ID chỉ giải quyết một phần vấn đề về tính tương minh và khả năng kiểm soát trong hệ thống IP mà nhà quản trị đang đối mặt trong môi trường Internet ngày nay. Xem xét nội dung dữ liệu của ứng dụng được phép đi vào hệ thống trở thành thách thức tiếp theo. Content-ID giúp giải quyết thách thức này để ngăn ngừa các mối hiểm họa (eg: anti-malware, anti-virus, IPS..), lọc URL và lọc dữ liệu.

Các sản phẩm chống tấn công hay ngăn ngừa các mối hiểm họa tại gateway hiện nay thường thực hiện lưu lại (proxy) toàn bộ tải trước khi scan virus, spyware, malware gây ra sự chậm trễ trong việc xủ lý. Do thiếu khả năng xử lý với tốc độ cao này buộc các doanh nghiệp phải dựa vào nhiều thiết bị riêng lẻ, gây ra khó khăn trong quản lý.

Palo Alto firewall tích hợp tính năng Threat Prevention vào firewall với các tính năng sau:

- Dò tìm và chặn viruses, spyware, worms, and lỗ hổng ứng dụng
- Kiểm soát việc truyền file hay thông tin nhạy cảm ra khỏi hệ thống
- Tốc độ xử lý cao.
- Giảm chi phí vận hành và quản trị với một giao diện quản lý

Công nghệ ngăn ngừa hiểm họa của firewall Palo Alto sử dụng công nghệ quét stream-based, khác với công nghệ file-based, thực hiện scan ngay khi packet đầu tiên đến. Đồng thời thay vì scan dữ liệu nhiều lần cho nhiều loại hiểm họa khác nhau, Palo Alto firewall phát triển format chữ ký đồng nhất (uniform signature) cho phép tìm ra nhiều loài hiểm họa (virus, malware, spyware, lỗ hổng ứng dụng..) trong một lần quét.

Ngoài ra, chức năng chống các lỗ hổng ứng dụng kết hợp nhiều tính năng IPS để ngăn ngừa các tấn công khai thác lỗ hổng bảo mật ở tầng ứng dụng và mạng như buffer overflow, DoS, port scan. Các cơ chế IPS gồm có:

- Protocol anomaly detection

- Stateful pattern matching
- Statistical anomaly detection
- Heuristic-based analysis
- Block invalid or malformed packets
- IP defragmentation and TCP reassembly

Công nghệ threat prevention của Palo Alto được thực hiện với độ trễ thấp và khả năng xử lý dữ liệu lớn nhờ vào công nghệ xử lý song song và tính năng phần mềm tiên tiến. Cơ chế threat prevention của Palo Alto đặt nặng vai trò nhận dạng ứng dụng trong việc truy tìm nguồn gốc các mối đe dọa một cách chính xác và hiệu quả.

3.3 Lọc URL Appliance-based URL filtering

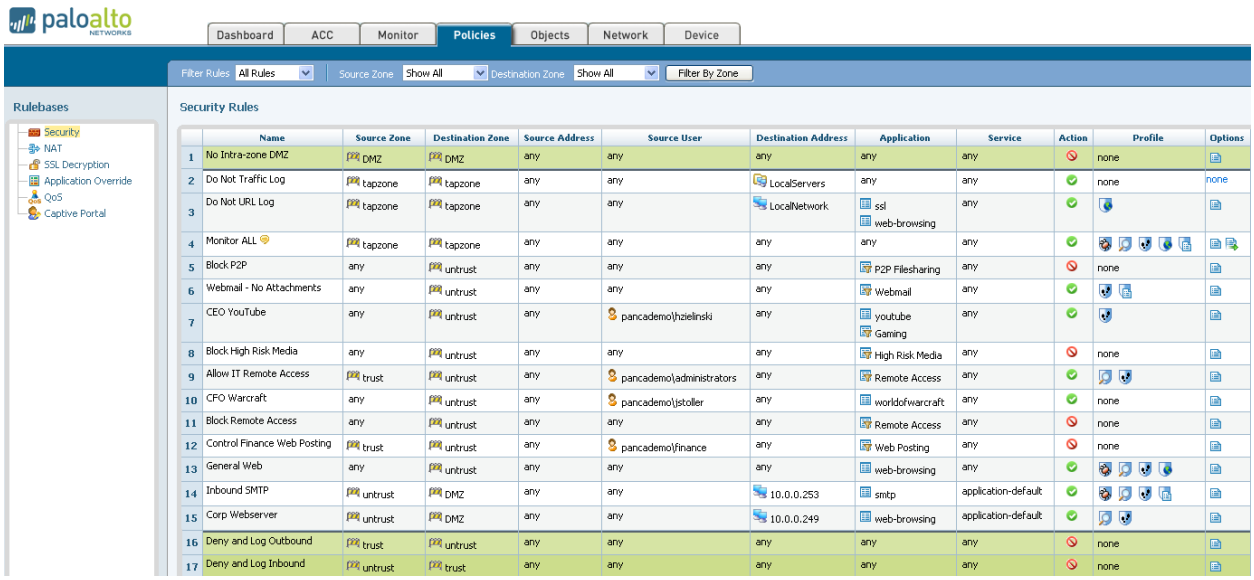
Theo dõi và kiểm soát hoạt động lướt web là yếu tố chính để bảo vệ hệ thống mạng của doanh nghiệp khỏi các nguy cơ về bảo mật và vi phạm các tiêu chuẩn. Tuy nhiên, phòng IT đang gặp rất nhiều khó khăn với các giải pháp trên chạy trên nền server hạn chế khả năng thực thi các điều luật. Để bảo vệ và kiểm soát hoạt động lướt web, phòng IT cần một số công cụ sau:

- Theo dõi hoạt động lướt web mà không ảnh hưởng đến thời gian đáp ứng và trải nghiệm của người dùng.
- Chính sách cho phép/ từ chối các trang web được thực hiện in-line theo thời gian thực.
- Cho phép tăng số lượng người dùng mà không phải

Palo Alto tích hợp cơ sở dữ liệu với hơn 20 triệu URL với trên 76 categories vào trong firewall cho phép kiểm soát việc lọc URL bổ sung cho khả năng kiểm soát ứng dụng dựa trên các điều luật bảo vệ doanh nghiệp từ việc tuân thủ một số các tiêu chuẩn cũng như tăng năng suất làm việc và giảm các nguy cơ gây hại đến nguồn lực công ty.
Nếu URL đi qua không nằm trong cơ sở dữ liệu URL trên box, firewall có thể hỏi từ một cơ sở dữ liệu khác với trên 180 triệu URLs. Sau đó URL đó có thể được lưu vào một cơ sở dữ liệu động và riêng biệt với 1 triệu URLs.

3.4 Chính sách kiểm soát an ninh

Nhận dạng ứng dụng App-ID kết hợp với User-ID và Contet-ID cho phép nhà quản trị kiểm soát: ai đang sử dụng ứng dụng nào; các mã độc, phần mềm gián điệp ứng dụng đó mang vào thông qua; thiết lập lọc url **chỉ bằng một bảng policy**. Đây là điểm khác biệt về mặt công nghệ so với các firewall truyền thống có thêm tính năng nhận dạng ứng dụng với nhiều policy khác nhau: policy cho firewall, policy cho ứng dụng, policy cho QoS, policy cho IPS, do đó thiếu sự liên kết.



Các thông tin App-ID, User-ID, và Content-ID mang lại một bức tranh toàn diện hệ thống mạng, cho phép đưa ra các policy cụ thể theo nhu cầu không chỉ đơn giản allow hay deny. Ví dụ như:

- Cho phép hay từ chối
- Cho phép nhưng scan virus, lỗ hổng hay các mối đe dọa khác
- Giải mã và kiểm tra
- Thực hiện QoS theo ứng dụng, người dùng, nhóm người dùng
- Thực hiện policy-based forwarding
- Cho phép/ từ chối một số chức năng của ứng dụng (eg: cho phép facebook chat, không cho phép facebook app…)

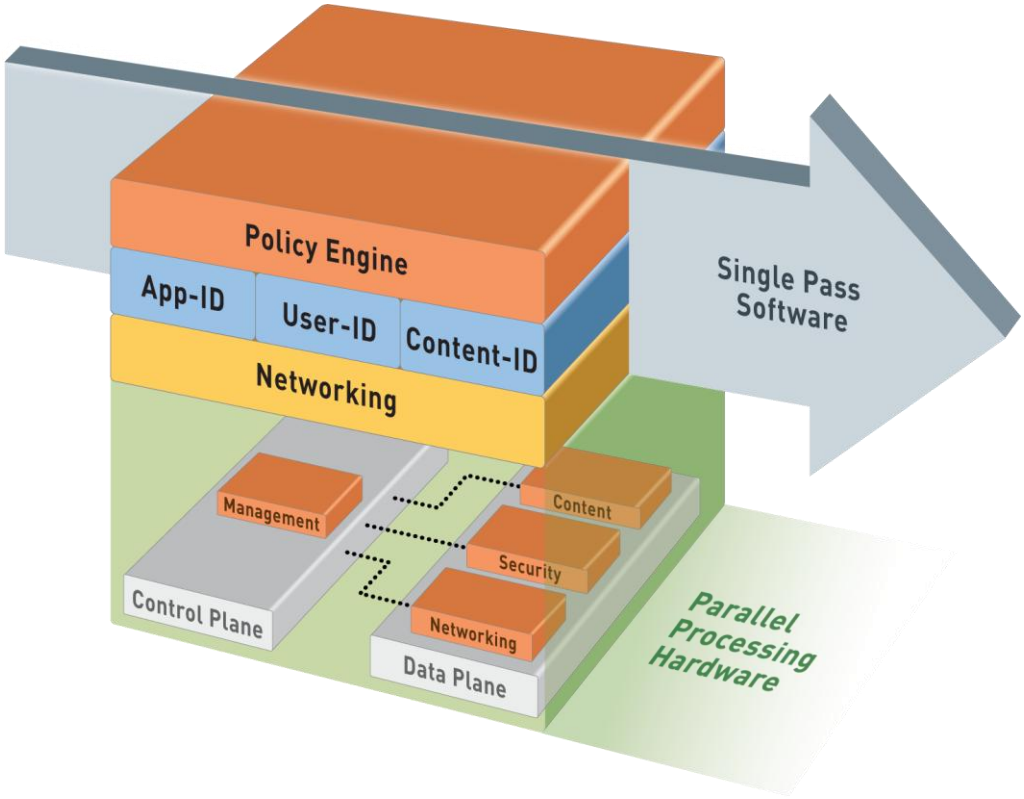
Sử dụng policy editor nhà quản trị có thể nhanh chóng tạo ra các chính sách cho firewall như:

- Cho phép nhóm Sale và Marketing sử dụng SAP và MS Exchange
- Chó phep nhóm IT dùng một số ứng dụng để quản trị thiết bị như ssh,telnet và RDP
- Chặn các ứng dụng không có ích như P2P file sharing, external proxies.
- Định nghĩa và áp các chính sách cho phép và Define and enforce a corporate policy that allows and inspects specific webmail and instant messaging usage.
- Kiểm soát các chức năng truyền file bên trong các ứng dụng, cho phép sử dụng ứng dụng nhưng cấm truyền file
- Xác định việc truyền các thông tin nhạy cảm như số credit card, số CMND đưới dạng text hoạc file format
- Triển khai các chính sách URL filtering đa cấp, ngăn cấm việc vào các trang web không phục vụ cho công việc, theo dõi các website đang nghi ngờ
- Thực hiên chính sách QoS cho phép sử dụng các ứng dụng media hay các ứng dụng sử dụng băng thông cao nhưng giới hạn băng thông và sự ảnh hương của nó đến các ứng dụng quan trong khác.

3.5 Kiến trúc Palo Alto

Trong nhiều năm, mục tiêu tích hợp threat prevention bao gồm IPS, anti-virus, anti-spyware vào firewall luôn được quan tâm để giảm thiểu số lượng thiết bị cũng như chi phí. Hiện nay, các firewall UTM hướng đến vấn đề tích hợp này. Tuy nhiên, các giải pháp này gặp phải vấn đề về khả năng xử lý của thiết bị. Chức năng firewall có thể xử lý với throughput rất lớn nhưng khi các tính năng an ninh khác được bật khả năng xử lý giảm xuống một cách đáng kể với độ trễ lớn.

Firewall thế hệ mới Palo Alto đưa ra kiến trúc "single pass parallel processing" nhằm giải quyết thách thức về mặt tích hợp và khả năng xử lý; sử dụng phương pháp "single pass" để xử lý gói tin cùng với phần cứng được thiết kế với mục đích xử lý song song.

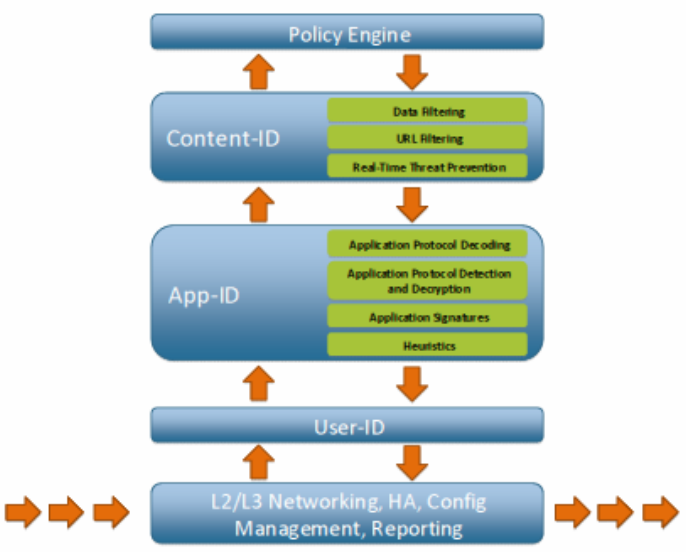


Single pass software:

Đây là kiến trúc xử lý duy nhất được thiết kế bởi Palo Alto. Phương pháp này thực hiện scan traffic và xử lý các tác vụ chỉ một lần bao gồm:

- Networking và management
- User-ID: map địa chỉ IP và active directory để xác định user hay group
- App-ID: kết hợp 4 cơ chế nhận dạng như trên. Quá trình nhận dạng này được thực hiện đồng thời với chức năng Content-ID để thực hiện scan và kiểm tra ứng dụng phù hợp với policy đặt ra.

- Content-ID: công cụ so sánh chữ ký (signature matching) với phần cứng tăng tốc sử dụng để scan lọc dữ liệu (eg: số thẻ tín dụng, số CMND, hay một số dữ liệu được định nghĩa trước), scan tìm threats (lỗ hổng bảo mật, virus, spyware) cộng với phân loại URL để thực hiện lọc URL.
- Policy engine: dựa trên các thông số về networking, management, User-ID, App-ID và Content-ID, policy engine sẽ áp các chính sách tương ứng. Đối với Palo Alto, chỉ có một bảng policy duy nhất giúp cho nhà quản trị dễ dàng trong việc thiết kế các chính sách quản lý.



Parallel processing hardware:

Phần cứng của Palo Alto được thiết kế để xử lý các tác vụ một cách song song, mỗi tác vụ sẽ được xử lý riêng biệt bởi từng CPU.

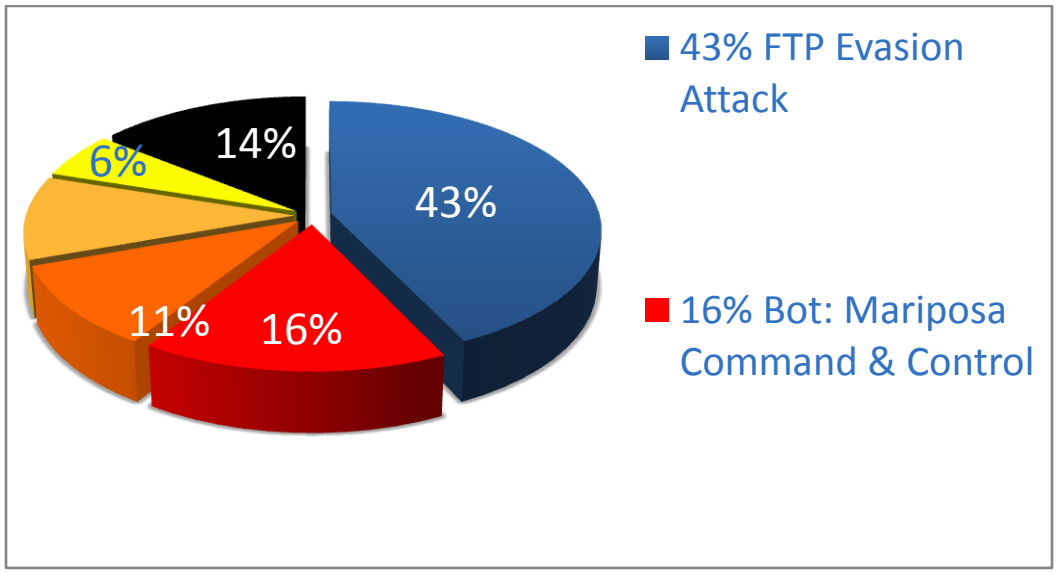
- Networking: flow control, routing, ARP, NAT…được thực hiện trên bộ xử lý dành riêng.
- User-ID, App-ID, và policy engine được xử lý bởi multicore security processor, với phần cứng được thiết kế để tăng tốc mã hóa, giải mã và giải nén.
- Content-ID thực hiện dò tìm chữ ký trên phần cứng FPGA với bộ nhớ dành riêng.
- Management: việc cấu hình, looging, và reporting được thực hiện thông qua bộ xử lý dành riêng cho control plane, riêng biệt với data plane để xử lý dữ liệu.

4 Report

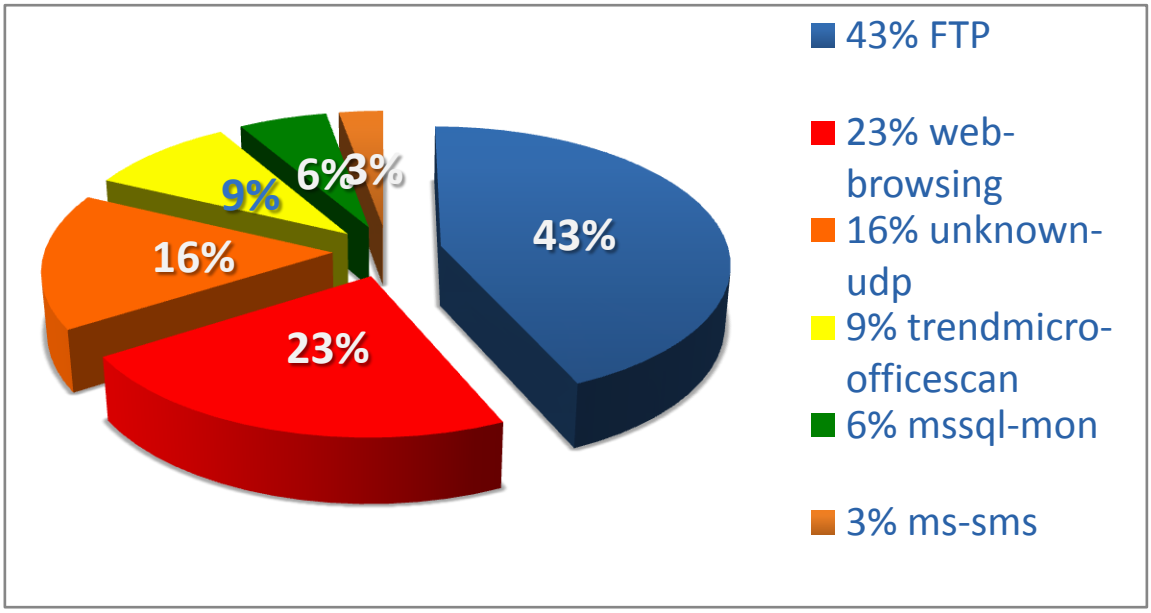
4.1 Application visibility report (AVR)

Là report mang tính thống kê chung cho toàn bộ hệ thống. Report này giúp cho nhà quản trị mạng cũng như những nhà quản lý IT có cái nhìn tổng quát về trong hệ thống bao gồm: các mối đe dọa mà hệ thống đang đối mặt, những ứng dụng nào gây ra nhiều nguy cơ cho hệ thống hay chiếm băng thông lớn…Sau đây là một số ví dụ:

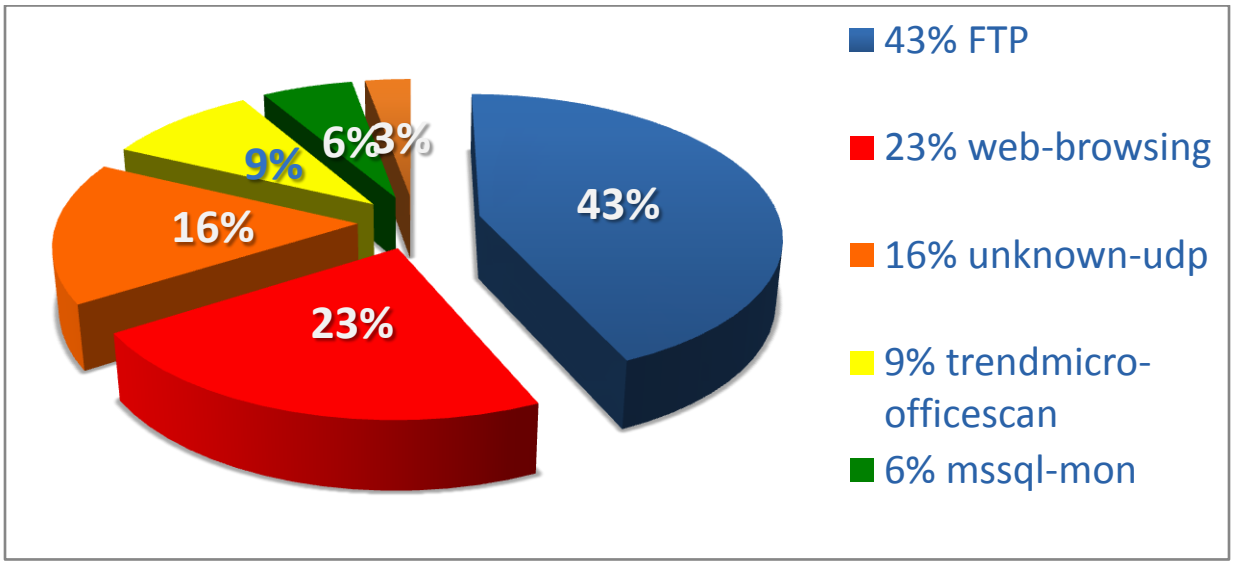
Critical severity threats



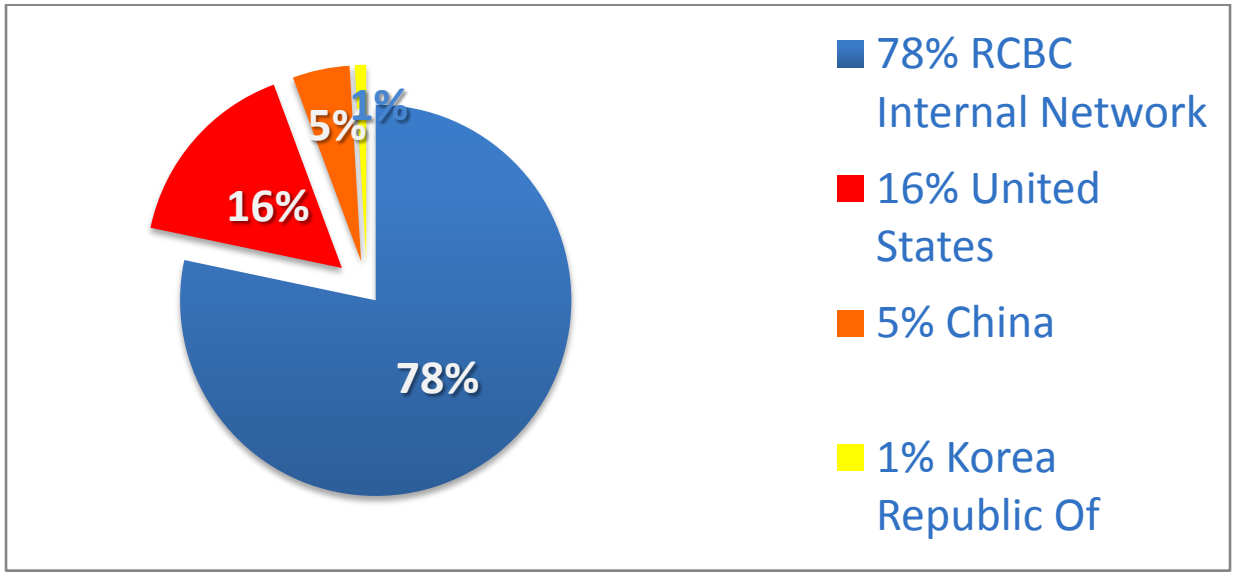
High severity threats



Top threats by application



Threats by country origin of Attacks



4.2 User activity report

Bên cạnh report mang tính tổng quát, Palo Alto cho phép xuất report chi tiết theo người dùng như một số ví dụ sau đây.

Application usage: cho phép report các loại ứng dụng mà người dùng đó sử dụng cùng với chi tiết về category, băng thông, số lượng session và mức độ nguy hiểm của ứng dụng đó.

Risk	Application	App Category	App Sub Category	App Technology	Sessions	Bytes
5	youtube-base	media	photo-video	browser-based	1.8k	2.7G
4	web-browsing	general-internet	internet-utility	browser-based	11.6k	1.7G
4	flash	general-internet	internet-utility	browser-based	517	1.0G
1	insufficient-data	unknown	unknown	unknown	24.6k	78.2M
2	google-toolbar	general-internet	internet-utility	client-server	315	16.5M
1	unknown-tcp	unknown	unknown	unknown	630	15.4M
5	bittorrent	general-internet	file-sharing	peer-to-peer	9.9k	4.5M
4	dns	networking	infrastructure	network-protocol	9.5k	2.8M
3	google-video	media	photo-video	browser-based	630	1.1M
2	google-safebrowsing	general-internet	internet-utility	browser-based	535	896.7k

Tóm tắt hoạt động lướt web theo category cùng với bandwidth mà các ứng dụng đó đã sử dụng.

Category	Count	Bytes
search-engines	2.9k	3.5G
streaming-media	2.5k	1.8G
content-delivery-networks	2.2k	27.6M
spyware-and-adware	1.8k	8.1M
sports	1.5k	19.9M
internet-portals	1.2k	2.9M
peer-to-peer	1.2k	1.4M
web-advertisements	1.1k	11.2M
business-and-economy	630	2.6M
unknown	315	490.5k
personal-sites-and-blogs	315	493.3k

Tóm tắt các website mà người dùng đó đã viếng thăm.

Host	Category	Count
i1.ytimg.com	content-delivery-networks	734
i2.ytimg.com	content-delivery-networks	520
ads.nba.com	sports	495
www.google.com	search-engines	470
i3.ytimg.com	content-delivery-networks	282
www.youtube.com	streaming-media	236
clients1.google.com	search-engines	235
tooltips.hotbar.com	spyware-and-adware	189
us.bc.yahoo.com	internet-portals	143
74.125.164.37	search-engines	141
i4.ytimg.com	content-delivery-networks	141
sports.yahoo.com	sports	96
thumbs.hotbar.com	spyware-and-adware	94

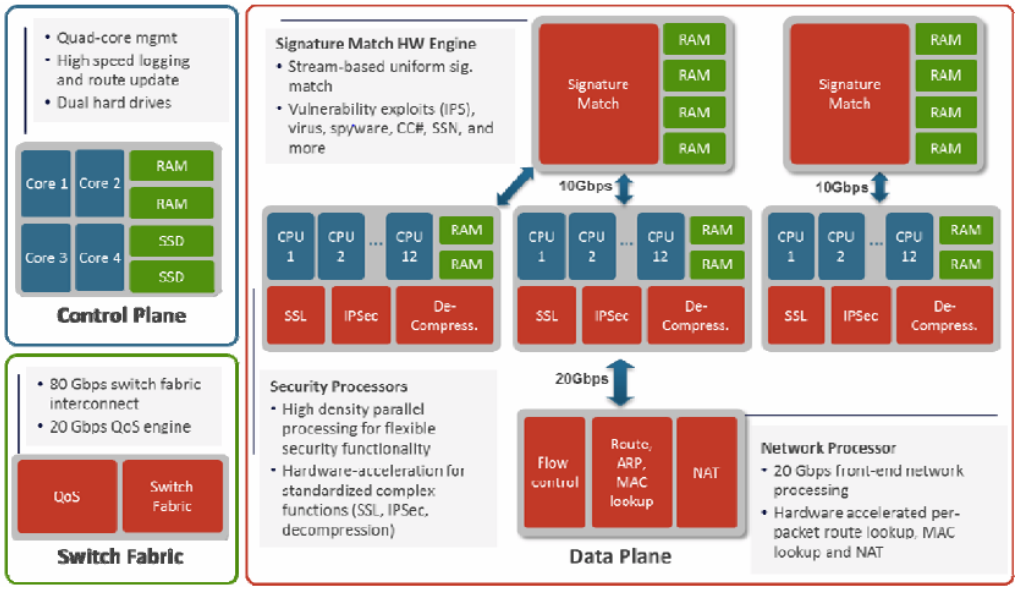
Tóm tắt chi tiết hoạt động của người dùng với chi tiết về thời gian, url, thể loại:

Receive Time	Application	URL	Category
2010/11/05 03:35:16	web-browsing	i1.ytimg.com/u/xnlfwroirrtysdgradujmg/watch_header.jpg?v=0	content-delivery-networks
2010/11/05 03:35:19	web-browsing	v24.lscache4.googlevideo.com/videoplayback?ip=0.0.0.0&sparams=i	streaming-media
2010/11/05 03:35:19	web-browsing	i1.ytimg.com/vi/tr32ahyboam/default.jpg	content-delivery-networks
2010/11/05 03:36:02	web-browsing	sports.yahoo.com/nba	sports
2010/11/05 03:36:06	web-browsing	ads.nba.com/html.ng/site=ynba&ynba_pos=300x250_rgt&ynba_rollup=	sports
2010/11/05 03:36:08	web-browsing	ads.nba.com/html.ng/site=ynba&ynba_pos=300x40_spon2&ynba_rollup	sports
2010/11/05 03:36:08	web-browsing	ads.nba.com/event.ng/type=count&clienttype=2&aseg=&amod=&adid=3	sports
2010/11/05 03:36:10	web-browsing	us.bc.yahoo.com/&u=13h3ktil5/n=q0wkbtgdjha-/c=698984.13077680.1	internet-portals
2010/11/05 03:36:10	web-browsing	us.bc.yahoo.com/b?p=pfirr2kipe4rvcgnskljjhvthpp6sepk1hiaae_x&t=	internet-portals
2010/11/05 03:36:58	web-browsing	i1.ytimg.com/vi/4mccigwax0i/default.jpg	content-delivery-networks
2010/11/05 03:36:58	web-browsing	i2.ytimg.com/vi/-aal7ixlrxw/default.jpg	content-delivery-networks
2010/11/05 03:36:58	web-browsing	i2.ytimg.com/vi/igtqszolz-4/default.jpg	content-delivery-networks
2010/11/05 03:37:07	web-browsing	i2.ytimg.com/vi/iepjvtvl0m4/default.jpg	content-delivery-networks
2010/11/05 03:37:08	web-browsing	www.youtube.com/get_video?video_id=_khb8jpqu94&t=vjvqa1ppcfmwi-	streaming-media
2010/11/05 03:37:08	web-browsing	v22.lscache2.googlevideo.com/videoplayback?ip=0.0.0.0&sparams=i	streaming-media

5 Hardware specification

5.1 PA-5000 series

Dưới đây là cấu trúc phần cứng của dòng PAN-5000.



Control Plane: sử dụng quad core Intel CPU với 4GB DRAM và ổ cứng dual solid state (SSD).

Data plane:

- 3 multi-core CPU để xử lý các tác vụ đòi hỏi khả năng tính toán cao như: SSL encryption/decryption, IPSec, decompression

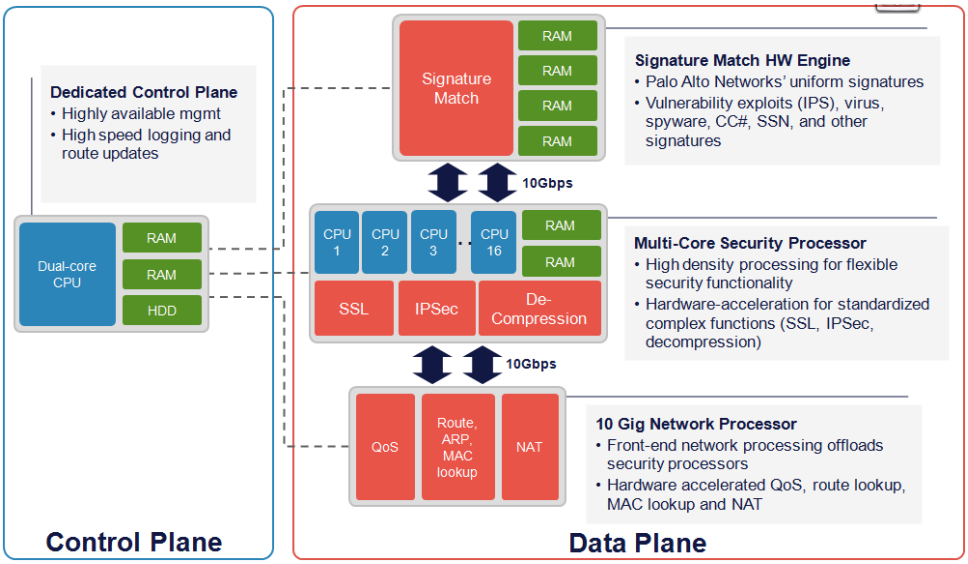
- Signature match engine với 2 FPGA có băng thông lớn để thực hiện scan threat, data filtering, App-ID..
- Network processor với băng thông 20Gbps

Mỗi block tác vụ đều có RAM dành riêng và kết nối với nhau với băng thông lớn (20Gbps, 10Gbps)

Firewall Palo Alto PA-5000 bao gồm 3 platforms PA-5020, PA-5050, PA-5060 được dành để triển khai như Internet gateway với tốc độ cao với các thông số:

KEY PERFORMANCE SPECIFICATIONS[1]	PA-5060	PA-5050	PA-5020
Firewall throughput	20 Gbps	10 Gbps	5 Gbps
Threat prevention throughput	10 Gbps	5 Gbps	2 Gbps
IPSec VPN throughput	4 Gbps	4 Gbps	2 Gbps
Max sessions	4,000,000	2,000,000	1,000,000
New sessions per second	120,000	120,000	120,000
IPSec VPN tunnels/tunnel interfaces	8,000	4,000	2,000
SSL VPN Users	20,000	10,000	5,000
Virtual routers	225	125	20
Virtual systems (base/max[2])	25/225	25/125	10/20
Security zones	900	500	80
Max number of policies	40,000	20,000	10,000

5.2 PA-4000 series



Control Plane: sử dụng dual-core Intel CPU với RAM và ổ cứng dual solid state (SSD).

Data plane:

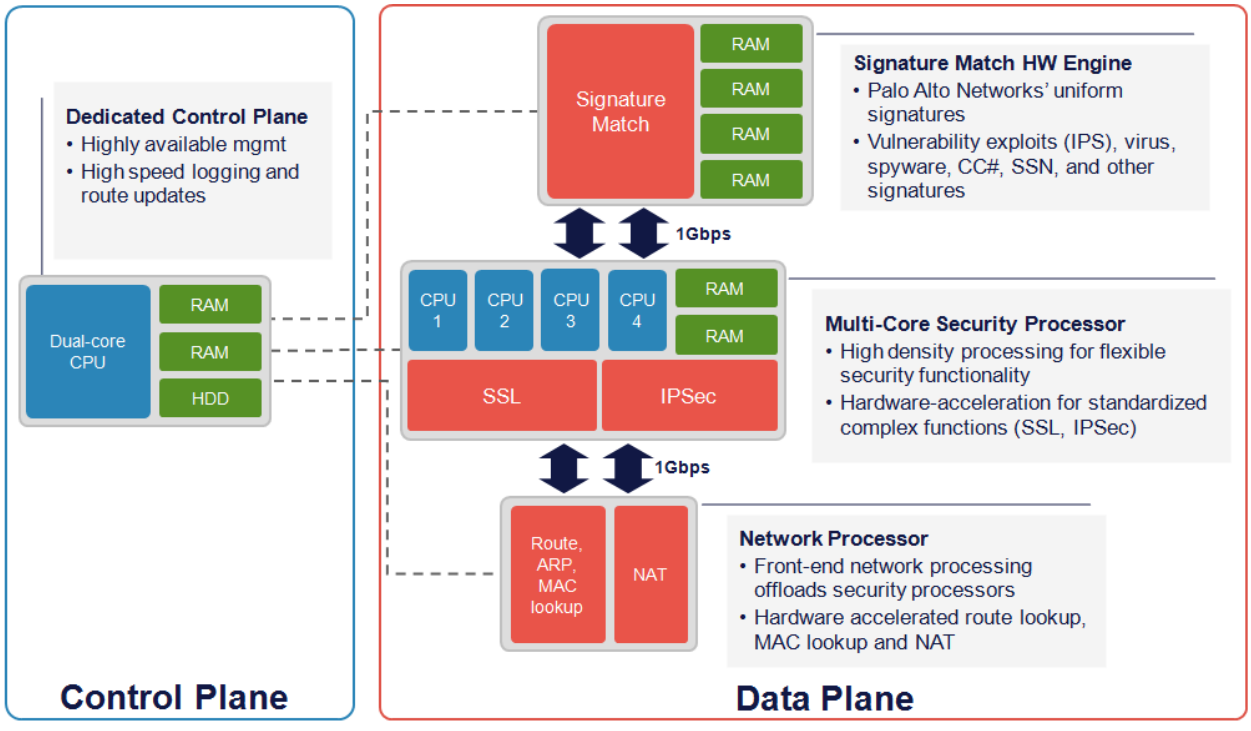
- 1 multi-core Security CPU để xử lý các tác vụ đòi hỏi khả năng tính toán cao như: SSL encryption/decryption, IPSec, decompression
- Signature match engine với 1 FPGA có băng thông lớn để thực hiện scan threat, data filtering, App-ID..
- 1 Network processor với băng thông 10Gbps

Mỗi block tác vụ đều có RAM dành riêng và kết nối với nhau với băng thông lớn (20Gbps, 10Gbps)

KEY PERFORMANCE SPECIFICATIONS	PA-4020	PA-4050	PA-4060
Firewall throughput	2 Gbps	10 Gbps	10 Gbps
Threat prevention throughput	2 Gbps	5 Gbps	5 Gbps
IPSec VPN throughput	1 Gbps	2 Gbps	2 Gbps
IPSec VPN tunnels/interfaces	2,000	4,000	4,000
New sessions per second	60,000	60,000	60,000
Max sessions	500,000	2,000,000	2,000,000

5.3 PA-2000 Series

Kiến trúc của dòng PA-2000:



Control Plane: sử dụng dual-core Intel CPU với RAM và ổ cứng HDD.

Data plane:

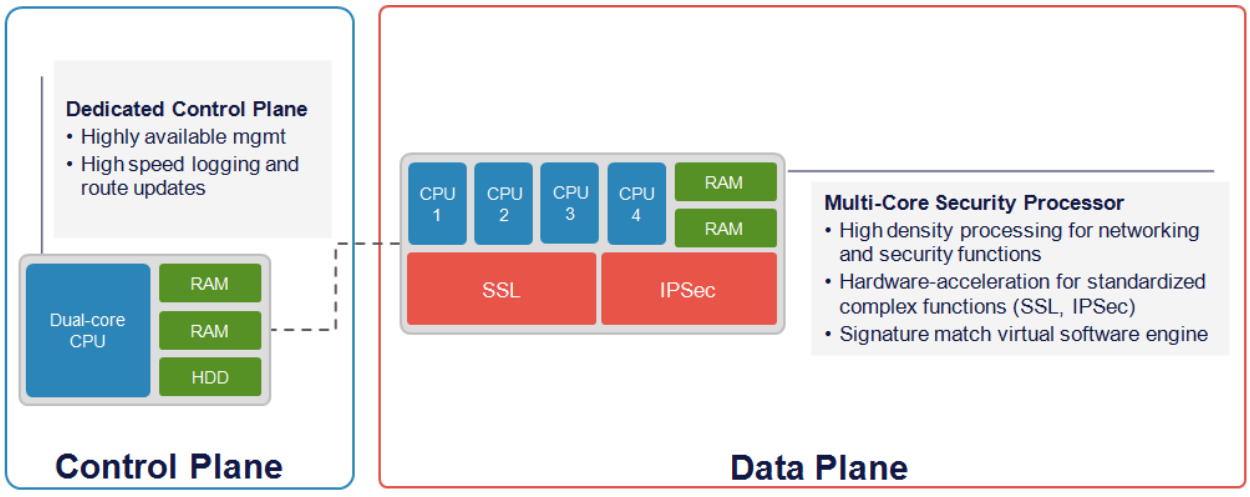
- 1 multi-core Security CPU để xử lý các tác vụ đòi hỏi khả năng tính toán cao như: SSL encryption/decryption, IPSec, decompression
- Signature match engine với 1 FPGA có băng thông lớn để thực hiện scan threat, data filtering, App-ID..
- 1 Network processor với băng thông 10Gbps

Mỗi block tác vụ đều có RAM dành riêng và kết nối với nhau với băng thông lớn (20Gbps, 10Gbps)

KEY PERFORMANCE SPECIFICATIONS	PA-2020	PA-2050
Firewall throughput	500 Mbps	1 Gbps
Threat prevention throughput	200 Mbps	500 Mbps
IPSec VPN throughput	200 Mbps	300 Mbps
IPSec VPN tunnels/interfaces	1,000	2,000
New sessions per second	15, 000	15,000
Max sessions	125,000	250,000

5.4 PA-500 Series

Kiến trúc của dòng PA-500:



- Kiến trúc Data plane va Control plane riêng biệt.
- Bộ xử lý network và signature matching engine ảo hóa trên the multi-core security processor.