EXCLUSIVE NETWORKS

paloalto NETWORKS

Palo Alto Networks Reference Guide

brought to you by

Exclusive Networks

Click to view

CONTENTS

EXCLUSIVE NETWORKS | paloalto NETWORKS

Contact your Palo Alto Networks Product Sales Specialists

SECURE THE ENTERPRISE

STRATA™ BY PALO ALTO NETWORKS

Threat Prevention - Next-Generation Firewall

Securing your enterprise starts with your firewall.

Palo Alto Networks industry-leading Next-Generation family of Firewalls have been redefining network security for 15 years, and counting. Eliminate known threats at every stage of an attack. Comprehensive exploit, malware, and command-and-control prevention for your enterprise. Gartner magic quadrant leaders for 8 consecutive years.

Physical Appliances

PA-Series

The full range of Palo Alto Networks Next-Generation Firewall physical appliances that are easy to deploy into your organisation's network and purposefully designed for simplicity, automation, and integration.

Virtualised Firewalls

VM-Series

Palo Alto Networks virtualised Next-Generation Firewalls protect your private and public cloud deployments with segmentation and threat prevention.

5G-ready firewalls

K2-Series

Palo Alto Networks K2-Series 5G-ready Next-Generation Firewalls are specifically developed for service providers' mobile network deployments.

EXCLUSIVE NETWORKS | paloalto NETWORKS

Contact your Palo Alto Networks Product Sales Specialists

QUALIFYING QUESTIONS FOR FIREWALL SOLUTIONS

STRATA BY PALO ALTO NETWORKS

- How are you protecting against known threats in your network?
- Do you have a solution in place to monitor east-west traffic?
- Are your firewall rules based on IPs and Ports?
- Is it complicated to align your business needs using those parameters?
- If I could show you a way of aligning your rules contextually, based on how your business runs, would you be interested?
- How's the management Experience when securing cloud, branch and mobile workers? Is it seamless and with feature parity?
- What's the process to ensure all your security tools work together to stop threats and don't conflict?
- What happens when you need to troubleshoot a ticket or investigate a threat across devices?
- There's a lot of talk about how attacks have become more sophisticated, how have you seen an impact on your team from this?
- Are you having trouble hiring enough cybersecurity employees? (Tip, check their open reqs on company site)
- How are your security tools using automation to reduce manual and repetitive tasks?

EXCLUSIVE NETWORKS | paloalto NETWORKS

Contact your Palo Alto Networks Product Sales Specialists

QUALIFYING QUESTIONS FOR URL FILTERING

STRATA™ BY PALO ALTO NETWORKS

URL Filtering enables you to safely use the web for business needs. Go beyond basic web filtering by identifying threats through a unique combination of static analysis augmented by machine learning.

- What systems are you implementing to automatically identify and prevent web based threats?
- Are you decrypting your web traffic? Are you able to selectively decrypt select web sites?
- Do your current web security tools work with your firewall to enable selective SSL decryption or prevent credential theft in real-time?
- Do they work with your IPS to dynamically enable stricter threat prevention?
- How has your organisation been impacted by phishing or spear phishing attacks in the past year?
- How are you protecting users from these threats?
- How many network security products do you currently manage?
- How much time do you spend integrating those products?
- What types of tasks do you wish your security staff had more time for?

QUALIFYING QUESTIONS FOR DNS SECURITY

STRATA BY PALO ALTO NETWORKS

A new subscription which is added to the NGFW alongside TP, WF, GP,URL etc. DNS Security service predicts and stops malicious domains from domain generation algorithm-based malware while quickly detecting data theft that employs DNS tunnelling with machine learning-powered analysis.

- Can you stop millions of malicious domains at once, in real-time?
- Are you inspecting DNS for data theft? Would you know if data was being ex-filtrated using DNS?
- What tools are you using to secure your DNS traffic today?
- What types of tasks do you wish your security staff had more time for?

QUALIFYING QUESTIONS FOR WILDFIRE

STRATA BY PALO ALTO NETWORKS

Automatically detect and stop unknown attacks. Identify new threats with advanced analysis, machine learning, and shared threat intelligence to stay ahead of attackers with automated protections.

- How many targeted attacks do you detect in your organisation?
- What is the current process to detect and stop unknown attacks?
- Do you have enough time and manpower to deal with these threats?
- How do you get access to effective threat related data?
- Do you have a team to analyse that threat data?
- How confident are you that you're catching all the threats targeting you?
- How many steps does it take to block an unknown threat?
- How many tools do you use to take a detection all the way to prevention?

QUALIFYING QUESTION FOR GLOBAL PROTECT

STRATA™ BY PALO ALTO NETWORKS

Every time users leave the building with their laptops or smartphones, they are bypassing the corporate firewall and associated policies that are designed to protect both the user and the network. GlobalProtect™ solves the security challenges introduced by roaming users by extending the same next-generation firewall-based policies that are enforced within the physical perimeter to all users, no matter where they are located.

- How are you protecting your staff, when they work from home, or off-site?
- Do you have a large mobile workforce?

QUALIFYING QUESTIONS FOR PANORAMA FOR MANAGEMENT

STRATA™ BY PALO ALTO NETWORKS

Panorama reduces network complexity with logical, functional device groups, simplifies network management with easy, global policy control, and reduces the time that threats linger on your network, with actionable data highlighting critical information for response prioritisation.

- How do you ensure your firewall policies are consistent across the enterprise?
- How do you ensure consistent firewall, threat prevention, web-filtering, and file policies across your network security tools?
- Are you confident that your firewall policies reflect your business policies?
- How's the management experience when securing cloud, branch and mobile workers? Is it seamless and with feature parity?
- Do you have centralised visibility into on premise and SaaS applications your users are accessing?

QUALIFYING QUESTIONS FOR SD-WAN

STRATA BY PALO ALTO NETWORKS

A software-defined wide area network, or SD-WAN, is a virtualised service that connects and extends enterprise networks over distances. SD-WAN monitors the performance of WAN connections and manages traffic in an effort to maintain strong speeds as well as optimise connectivity. Security and SD-WAN must converge. With security natively integrated with SD-WAN, you can connect your branch offices without compromising on security.

- How are you optimising the middle and last mile of your end-to-end network to ensure optimal end-user experience?
- Are there any regional/branch expansions or merger projects on the roadmap?
- What kind of impact would it have if you could speed up branch turn-up times?
- How concerned are you about configuring and managing the interconnect yourself?
- How do you plan on integrating your SD-WAN security into the rest of your security infrastructure?
- Is vendor consolidation and simplifying your security infrastructure a current initiative at your organisation?

QUALIFYING QUESTIONS FOR AUTOFOCUS THREAT INTELLIGENCE

STRATA™ BY PALO ALTO NETWORKS

Palo Alto Networks AutoFocus™ threat intelligence service re-imagines how security teams protect their organisations from unique, targeted attacks. The hosted security service provides the intelligence, analytics, and context required to understand which attacks require immediate response, as well as the ability to make indicators actionable and prevent future attacks.

- Do your security teams need to quickly prioritise and respond to attacks?
- Are your current methods complex and manual?
- Do your security teams need to quickly prioritise and respond to attacks?
- Are your current methods complex and manual?
- How important is threat intelligence to your business?

QUALIFYING QUESTIONS FOR IOT, ZINGBOX

STRATA™ BY PALO ALTO NETWORKS

Zingbox's cloud-based service uses AI and machine learning technologies to help organisations discover, identify, secure and optimise unmanaged devices. With the addition of Zingbox, Palo Alto Networks now offers IoT security with best-in-class visibility and automated real-time threat mitigation.

- Are you struggling to manage the complex IoT lifecycle in your business?
- Are you able to to meet the challenge and extend IT best practices to IoT your devices?

QUALIFYING QUESTIONS FOR PRISMA

Prisma Access

Prisma Access Secure Access Service Edge (SASE) enables mobile users and branch offices to securely access the cloud through a scalable, cloud-delivered security architecture. This means you don't have to worry about sizing and deploying firewalls at each branch office. Remote Access VPN is not designed to support cloud applications with Prisma Access. It uses cloud infrastructure to connect users to both cloud apps and the data center.

- Growth plan for the end user? Do you provide consistent security to your mobile and branch users?
- Do you have large volumes of remote users or remote branches?
- Are you looking to reduce your hardware footprint?

Prisma Cloud

Prisma Cloud (formally Redlock and Evident) Comprehensive threat protection, governance, and compliance offering. Ensuring data and workloads are visible and secure across GCP, AWS and Microsoft Azure. Moving away from private cloud/data centre.

- Do you know what you are storing in the cloud, and are you GDPR compliant?
- Do you use the public cloud?
- Container security - Do your SecOps teams have visibility into your DevOps teams?
- Can you maintain consistent security in the cloud as well as on the network?
- Can you be sure you are compliant and have consistent security policies when using the public cloud?

QUALIFYING QUESTIONS FOR PRISMA

Prisma SaaS

Prisma SaaS (formally Aperture) addresses your cloud access security broker needs (CASB), prevents data loss and disruptions through granular application visibility, monitoring and threat protection. Offering in-line and API-based protection working together to minimise the range of cloud risks that can lead to breaches.

- How are you managing data that your users are accessing through SaaS applications? How do you control the use of unauthorised applications?
- SaaS apps such as Office 365, Dropbox, SFDC. Can you control access from unmanaged devices?

VM Series

VM-Series NGFWs enable secure transformation of traditional data centers to software-defined data centers, or SDDCs, through tight integration with data centre infrastructure partners. VM-Series NGFWs simplify security workflows with automation and prevent successful cyberattacks that move laterally across a data center.

- Do you have micro-segmentation/network segmentation projects
- Do you have software-defined networking projects within data centres (with VMware NSX, Cisco ACI, Nuage VSP, Juniper Contrail, BigSwitch BIG-IP or OpenStack)
- Do you need visibility into east-west traffic within your data centre and public cloud?

QUALIFYING QUESTIONS FOR CORTEX

Cortex XDR

Break detection and response silos to stop sophisticated attacks by stitching together endpoint, cloud and network data. It builds a profile around the machine to know and learn the behaviours.

Unique in the breadth and depth of its endpoint protections:

- Stops malware, exploits and ransomware by observing attack techniques and behaviours
- Uses machine learning and AI to automatically detect and respond to sophisticated attacks
- Includes WildFire® malware prevention service to improve accuracy and coverage
- Harnesses Cortex XDR™ detection and response to speed, alert triage and incident response by providing a complete picture of each threat and its root cause, automatically
- Coordinates enforcement with network and cloud security to prevent successful attacks
- Provides a single lightweight agent for protection and response
- Protects endpoints while online and offline, on network and off
- What is your Security Analysts' approach to investigating and finding the root cause of incidents?
- And how are they managing visibility & finding a resolution?
- Are you currently using next gen endpoint protection/antivirus?
- How do you detect and respond to threats today?
- What do you have in place to find an active attacker or a malicious insider in your network?
- What percentage of security alerts can you investigate today?
- How long does it take you to triage and investigate alerts?
- How many alerts do you receive a week?
- What is a typical process to investigate an alert?
- What are your greatest security operations challenges?
- Do you have enough staff to handle all your security alerts?
- Do you have any active endpoint detection and response (EDR), or network traffic analysis projects?
- Do you proactively hunt threats?
- Do you have a dedicated security operations team?
- How do you handle alerts and investigations?
- How many people are in your security team?

Recommendation: Organisations that do not have a dedicated team to investigate alerts are not good candidates for Cortex XDR. Refer to an MDR partner.

- What is your stance on cloud-delivered security?

EXCLUSIVE NETWORKS | paloalto NETWORKS

Contact your Palo Alto Networks Product Sales Specialists

QUALIFYING QUESTIONS FOR CORTEX

Cortex Data Lake

AI-based continuous security operations platform, designed for massive scale as a cloud service. Cortex Data Lake effortlessly centralises all data and global threat intelligence across your entire security infrastructure.

Palo Alto Networks products send rich network, endpoint and cloud data to the Data Lake. This is made accessible to Palo Alto Networks & Third Party applications through the Cortex Hub.

Cortex XSOAR

Security, Orchestration, Automation and Response (SOAR) combines full case management, intelligent automation serving security teams across the incident lifecycle. The goal is to reduce alert fatigue in the SOC and improve analyst productivity to enable more efficient security operations.

- How are you automating your security responses? Is your SOC team flooded with alerts?

FACTS & FIGURES

Palo Alto Networks & Prisma Public Cloud

Palo Alto Networks

- 85 of the fortune 100 companies use our products and trust us
- Gartner top right for 8 consecutive years for the NGFW
- 2 consecutive years at the top of Zero Trust leadership rankings
- 65,000 customers in 150+ countries
- 80% of data breaches are caused by someone you let in
- 100% of evasions blocked earning the highest Security Effectiveness score
- The number of devices connected to the Internet is exploding; IDC forecasts up to 41.6 billion by 2025. As your data spreads ever further, there are more opportunities for attacks; legacy security systems are becoming too complex to manage. Our prevention-based architecture simplifies your organisation's security posture through an integrated solution
- It is estimated that there will be a shortfall of around 3.5 million cyber security professionals by the year 2021

Prisma Public Cloud

- By 2022, 60% of server workloads will use application control in lieu of antivirus, which is an increase from 35% at YE18
- Through 2020, due to the immaturity of incumbent CWPP offerings, 70% of organisations will use a different CWPP offering for container and serverless protection than they use for virtual machine protection

EXCLUSIVE NETWORKS | paloalto NETWORKS

Contact your Palo Alto Networks Product Sales Specialists

FACTS & FIGURES
Firewall & XDR

Firewall

- Through 2023, 99% of firewall breaches will be caused by firewall misconfigurations, not firewall flaws - Gartner
- 100% of evasions blocked earning the highest Security Effectiveness score
- Enabled by new application technologies, software releases have moved from once or twice per year to many times per day. New applications can have components that run on-premises, in the cloud and across hybrid clouds at the same time
- Because of the technology we invented, we're able to dramatically reduce network sprawl in companies.
- We typically save our clients 65% in capital costs and 80% in operational costs

XDR

- It typically takes organisations 197 days to identify and 69 days to contain threats
- To secure their networks, many organisations have deployed siloed tools. Tools like Endpoint Detection and Response (EDR), Network Traffic Analysis (NTA), User Entity Behavioral Analytics (UEBA) and many others, in fact larger enterprises have often deployed products from 50 or 60 or 70 different vendors. These tools don't work with one another to stop attacks. Instead, they generate large volumes of alerts in their own unique log formats. In fact, organizations receive 174,000 alerts per week but can only investigate 7% of them
- 50x reduction in alert volume, 8x faster investigations and 44% lower cost

(Reduce alerts by 50 times: Avoid alert fatigue with a game changing unified incident engine that intelligently groups related alerts. Investigate eight times faster: Verify threats quickly by getting a complete picture of attacks with root cause analysis. Maximise ROI: Use existing infrastructure for data collection and control to lower costs by 44%)

FACTS & FIGURES

XSOAR & SASE - Secure Access Service Edge

XSOAR

- Security teams review 12,000 alters per week on average. High volume of false positives is a related challenge
- Security analysts are tough to hire, train and retain. It takes 8 months to train new security analysts and 25% of them leave within 2 years
- Over 50% of security teams polled either don't have processes, or rarely update the processes they have. This leads to increased error rate, quality variance and lack of compliance
- Esri used Demisto playbooks and reduced alert volume by 95%
- An app development customer was able to reduce average times for a process from 4 hours to 10 minutes using a Demisto playbook

Secure Access Service Edge

- By 2023, 20% of enterprises will have adopted SWG, CASB, ZTNA and branch FWaaS capabilities from the same vendor up from less than 5% in 2019
- By 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at year-end 2018
- By 2025, at least one of the leading IaaS providers will offer a competitive suite of SASE capabilities
- Flexibility: With a cloud-based infrastructure, you can implement and deliver security services such as threat prevention, web filtering, sandboxing, DNS security, credential theft prevention, data loss prevention and Next-Generation Firewall policies
- Cost savings: Instead of buying and managing multiple point products, utilising a single platform will dramatically reduce your costs and IT resources
- Reduced complexity: You can simplify your IT infrastructure by minimising the number of security products your IT team has to manage, update and maintain, consolidating your security stack into a cloud-based network security service model

INDUSTRY SPECIFIC PAIN POINTS

Finance

- Support new technology innovations, such as mobile deposits, multi-channel customer service, social media engagements, and broader IT trends like the virtualisation of the data centre, cloud computing, and internet as a wide area network (WAN)
- Enable safe access to customer financial data from a myriad of entry points, including retail bank branches, partner facilities, client desktops, mobile devices
- Ensure compliance with FINRA, SEC, OCC, EBA, MAS and other regulations over financial transactions and sensitive customer data
- MIFID2 = customer data segmentation - is normally a good driver for companies to leverage public cloud
- Established organisations are having to be innovative and drive agility due to threat of FinTech companies who are competing and stealing much more market share than ever before
- Open Banking standards, set by CMA- Banking applications have to be made to integrate with one another
- General theme about aggregating large customer data insights to drive greater upsell / Xsell opportunities (not just limited to finance industry)

Higher Education

- Phishing / Social engineering
- Procedures not followed by staff
- Legitimate credentials used against the university
- Ransomware
- Losing control of data in the cloud
- Lack of joined up visibility

Legal

- Data security
- Remote workers / big perimeter
- Their own customers impacting their tech stack / security (not being able to use cloud etc.)

EXCLUSIVE NETWORKS | paloalto NETWORKS

Contact your Palo Alto Networks Product Sales Specialists

INDUSTRY SPECIFIC PAIN POINTS

Manufacturing

- Industry 4.0 - digitisation of manufacturing e.g. high degree of automation from upstream to downstream (e2e)
- Robotic manufacturing & warehouse management
- SOC and OT (operational technology e.g. plant) SOC merging
- Erosion of air gapped networks between plant and rest of network - caused by machines needing to be internet connected and ERP platforms requiring access
- Monitored maintenance: manufacturing machines feeding telemetry data back to vendors to monitor, reducing the risk of downtime (introduces new risks)

Retail

- PCI / Payments
- Single view of the customer - siloed data
- Omnichannel - seamless experience across store / web / phone
- Harnessing big data analytics
- In-store technology to optimise retail opportunities

Healthcare

- Ensure compliance with HIPAA, PCI and other regulations impacting patient data, medical equipment, and credit card transactions
- Enable safe access to patient data from a myriad of entry points, including hospitals, clinics, insurers, doctors' home offices, affiliate facilities, mobile devices, and more
- Detect and block threats; investigate cyber incidents
- Protect Windows PCs that are difficult to patch

NHS

- Budget
- Patching
- Governance
- Connectivity - SD-WAN
- Vulnerabilities on medical devices
- Lack of resources
- Lack of security

EXCLUSIVE NETWORKS | paloalto NETWORKS

Contact your Palo Alto Networks Product Sales Specialists

WHITE SPACE

SECURE THE ENTERPRISE

- Threat Prevention Next-Generation Firewall
- URL Filtering
- DNS Security Service
- Wildfire
- Global Protect
- Panorama for Management
- SD-WAN
- Autofocus Threat Intelligence
- IoT, Zingbox

SECURE THE CLOUD

- Prisma Access
- Prisma Cloud
- Prisma SaaS
- VM-Series

SECURE THE FUTURE

- Cortex Data Lake
- Cortex XDR
- XSOAR
- Zingbox

EXCLUSIVE NETWORKS | paloalto NETWORKS

Contact your Palo Alto Networks Product Sales Specialists

MEET THE TEAM

Contact your Palo Alto Networks Product Sales Specialists:

Lars Juul

Vendor Manager

Contact Lars

Ken Nielsen

Sales Engineer

Contact Ken

Betina Persson

Partner Account Manager

Contact Betina

Lone de Visme

Partner Account Manager

Contact Lone

Anne Mette Andersen

Inside Sales

Contact Anne Mette

Maja Radojevic

Inside Sales

Contact Maja

Anders Nørregaard

General Manager

Contact Anders

Monica Jernberg

Finance

Contact Monica

Jette Andersson

Marketing

Contact Jette

Exclusive Networks Denmark, Tuborg Boulevard 2, st.
2900 Hellerup **Tel:** +45 70 234 235
sales_dk@exclusive-networks.com
www.exclusive-networks.com/dk/