Juniper Networks | Federal

How Juniper Networks is Meeting Zero Trust

Zero Trust Capabilities Matrix

Networks are one of the core pillars of the Zero Trust framework.

Juniper Networks has a long history of working with the U.S. federal government and military.

With the proliferation of cyberattacks worldwide continuing to increase, the Department of Defense (DoD) has mandated itself and the industry to meet Zero Trust Architecture (ZTA) and other National Institute of Standards and Technology (NIST) requirements.

This capabilities matrix helps map how Juniper Networks meets these requirements.

Juniper & ZTA Pillars 5 and 6

Zero Trust Pillar	Section	Response
Network & Environment	5.1	For Juniper Networks' Automated WAN portfolio, **Juniper® Paragon Automation** provides automated, consistent, and reliable network trust and compliance that can verify, confirm, and quantify the trust aspects of the network, making it easier for network operators to run trustworthy networks.
Network & Environment	5.2	For Juniper Networks' Automated WAN portfolio, Juniper Paragon Automation provides intent-based, TPM 2.0-secured device onboarding, services instantiation, and device and network observability and management. Closed-loop remediation is possible via advanced analytics integrated into real-time decision making for congestion avoidance. Separation of control and data plane are central to the architecture of every Juniper router. Open, standardized APIs (like NETCONF and REST) are used for the secure exchange of configuration, management, and telemetry.
Network & Environment	5.3	Juniper Networks has a set of validated designs (**JVDs**) that encompass data center, campus and branch, and edge uses cases (Industrial Edge, Cloud Connect Edge, Private Network Edge, Data Center Edge, and Data Center Interconnect (DCI)). Each of these JVDs define the route, switch, and security capabilities to address macrosegmentation use cases with curated and validated designs.
Network & Environment	5.4	In additional to the JVDs described above, which are very much appropriate to the macrosegmentation needs of Zero Trust networks, Juniper Networks is able to provide microsegmentation in virtualized environments at the VM and container levels. Juniper's vSRX FW and **cSRX** (containerized) FW are both full-function, next-generation FWs, providing both North-South and East-West cyber protection. The cSRX Container Firewall delivers a complete virtualized solution with advanced security and automated life cycle and policy management. The cSRX empowers security professionals to deploy and scale firewall and advanced security detection and prevention in highly dynamic container environments. **Juniper Paragon Automation** is a modular portfolio of cloud-native software applications that helps operators simplify their network operations by eliminating manual tasks, processes, and workflows that are often repetitive and prone to human error. Paragon Automation delivers closed-loop automation to translate business intent into service performance across the entire service delivery life cycle. Paragon Automation builds on Juniper Networks' existing automation portfolio to meet the most pressing challenges of current and next-generation networks and services. **Paragon network automation** platform and products, powered by AI and ML, are designed to provide end users with an assured service experience. **Paragon Active Assurance** is a programmable, active test and monitoring solution for physical, hybrid, and virtual networks that verifies application and service performance. **Paragon Insights** is a network health and diagnostic solution that provides operational intelligence across all service provider, cloud, and enterprise network domains, from network access to servers in the data center. **Paragon Network Trust and Compliance** provides automated, consistent, and reliable network trust and compliance that can verify, confirm, and quantify the trust aspects of the network, making it easier for network operators to run trustworthy networks. The cloud-based automation solution measures the risk of integrity impairment and trust posture of network infrastructure. In parallel, it provides insight and nonintrusive validation of trustworthiness and reliability throughout the network.
Automation & Orchestration	6.3 & 6.4	Recent advances in generative AI catapulted AI and machine learning (ML) into the corporate, federal, service provider, and cloud provider spotlight. **Data centers** are the engines behind AI, and data center networks play a critical role in interconnecting and maximizing the utilization of costly GPU servers. AI training, measured by job completion time (JCT), is a massive parallel processing problem. A fast and reliable network fabric is needed to get the most out of your expensive GPUs. The right network is key to optimizing ROI and the formula is simple: design the right network, save big on AI applications.
Automation & Orchestration	6.5	**Juniper's Security Director** software offers centralized security policy management, automation, and response across physical, virtual, and containerized firewalls. Install on-prem and operate through a modern and centralized web-based interface.
Automation & Orchestration	6.6	Juniper Networks uses standardized applications programming interfaces across all products and control point software. Examples include: **Paragon Pathfinder API Documentation** **Threat Intelligence Open API** **Junos® OS REST API Guide**

Pillar 5: Network & Environment

JUNIPER NETWORKS | Federal

Capability	Capability Description	Impact to ZT	Associated Activities	Juniper Products/Solutions
5.1 Data Flow Mapping	DoD organizations reconcile data flows by gathering, mapping, and visualizing network traffic data flows and patterns to ensure authorized access and protection for network and DAAS resources, specifically tagging programmatic (e.g., API) access when possible.	Sets the foundation for network segmentation and tighter access control by understanding data traffic on the network	*Define Granular Control Access Rules & Policies Pt. 1 *Define Granular Control Access Rules & Policies Pt. 2	For Juniper Networks' Automated WAN portfolio, Juniper **Paragon Automation**, provides automated, consistent, and reliable network trust and compliance that can verify, confirm, and quantify the trust aspects of the network, making it easier for network operators to run trustworthy networks.
5.2 Software-Defined Networking (SDN)	DoD organizations define API decision points and implement SDN programmable infrastructure to separate the control and data planes and centrally manage and control the elements in the data plane. Integrations are conducted with decision points and segmentation gateway to accomplish the plane separation. Analytics are then integrated to real-time decision making for access to resources.	Enables the control of packets to a centralized server, provides additional visibility into the network, and enables integration requirements	*Define SDN APIs *Implement SDN Programmable Infrastructure *Segment Flows into Control, Management, and Data Planes *Network Asset Discovery & Optimization *Real-Time Access Decisions	For Juniper Networks' Automated WAN portfolio, Juniper Paragon Automation, provides intent-based, TPM 2.0-secured device onboarding, services instantiation, and device and network observability and management. Closed loop remediation is possible via advanced analytics integrated into real-time decision making for congestion avoidance. Separation of control and data plane are central to the architecture of every Juniper router. Open, standardized APIs, like NETCONF and REST, are used for secure exchange of configuration, management, and telemetry.
5.3 Macro-segmentation	DoD organizations establish network boundaries and provide security against networked assets located within an environment by validating the device, user, or NPE on each attempt of accessing a remote resource prior to connection.	Network segmentation is defined by a large perimeter to enable resource segmentation by function and user type	*Datacenter Macrosegmentation *B/C/P/S Macrosegmentation	Juniper Networks has a set of Validated Designs (**JVDs**) that encompass data center, campus and branch, and edge uses cases (Industrial Edge, Cloud Connect Edge, Private Network Edge, Data Center Edge, and Data Center Interconnect (DCI)). Each of these JVDs defines the route, switch, and security capabilities to address macrosegmentation use cases with curated, validated designs.
5.4 Micro-segmentation	DoD organizations define and document network segmentation based on identity and/or application access in their virtualized and/or cloud environments. Automation is used to apply policy changes through programmatic (e.g., API) approaches. Lastly, where possible, organizations will utilize host-level process microsegmentation.	Network segmentation enabled by narrower and specific segmentation in a virtualized environment via identity and/or application access, allowing for improved protection of data in transit as it crosses system boundaries (e.g., in a coalition environment, system high boundaries) and supported dynamic, real-time access decisions and policy changes	*Implement Microsegmentation *Application & Device Microsegmentation *Process Microsegmentation *Protect Data In Transit	In addition to the JVDs described above, which are very much appropriate to the macrosegmentation needs of Zero Trust networks, Juniper Networks is able to provide microsegmentation in virtualized environments at the VM and container levels. **Juniper's vSRX FW and cSRX (containerized) FW** are both full function, next-generation FWs, providing both North-South and East-West cyber protection. The cSRX Container Firewall delivers a complete virtualized solution with advanced security and automated life cycle and policy management. The cSRX empowers security professionals to deploy and scale firewall and advanced security detection and prevention in highly dynamic container environments.

Pillar 5: Network & Environment–Activities

ID	Activity Name	Description	Outcomes
5.1.1	Define Granular Control Access Rules & Policies Pt. 1	The DoD enterprise working with the organizations creates granular network access rules and policies. Associated Concept of Operations (ConOps) are developed in alignment with access policies and ensure future supportability. Once agreed upon, DoD organizations will implement these access policies into existing network technologies (e.g., Next-Generation Firewalls, Intrusion Prevention Systems) to improve initial risk levels.	Provide technical standards; Develop concept of operations; Identify communities of interest
5.1.2	Define Granular Control Access Rules & Policies Pt. 2	DoD organizations utilize data tagging and classification standards to develop data filters for API access to the SDN infrastructure. API decision points are formalized within the SDN architecture and implemented with non-mission/task-critical applications and services.	Define data tagging filters for API infrastructure
5.2.1	Define SDN APIs	The DoD enterprise works with the organizations to define the necessary APIs and other programmatic interfaces to enable SDN functionalities. These APIs will enable Authentication Decision Point, Application Delivery Control Proxy, and Segmentation Gateways automation.	SDN APIs are standardized and implemented; APIs are functional for AuthN Decision Point, App Delivery Control Proxy, and Segmentation Gateways
5.2.2	Implement SDN Programmable Infrastructure	Following the API standards, requirements, and SDN API functionalities, DoD organizations will implement SDN infrastructure to enable the automation of tasks. Segmentation Gateways and Authentication Decision Points are integrated into the SDN infrastructure, along with output logging into a standardized repository (e.g., SIEM, Log Analytics), for monitoring and alerting.	Implemented Application Delivery Control Proxy; Established SIEM logging activities; Implemented User Activity Monitoring (UAM); Integrated with Authentication Decision Point; Implemented Segmentation Gateways
5.2.3	Segment Flows into Control, Management, and Data Planes	Network infrastructure and flows are segmented either physically or logically into control, management, and data planes. Basic segmentation using IPv6/VLAN approaches is implemented to better organize traffic across data planes. Analytics and NetFlow from the updated infrastructure is automatically fed into operations centers and analytics tools.	IPv6 Segmentation; Enable automated NetOps information reporting; Ensure configuration control across enterprise; Integrated with SOAR
5.2.4	Network Asset Discovery & Optimization	DoD organizations automate network asset discovery through the SDN infrastructure, limiting access to devices based on risk-based methodical approaches. Optimization is conducted based on the SDN analytics to improve overall performance and provide necessary approved access to resources.	Technical refreshment/technology evolution; Provide optimization/performance controls
5.2.5	Real-Time Access Decisions	SDN infrastructure utilizes cross-pillar data sources, such as user activity monitoring, entity activity monitoring, enterprise security profiles, and more for real-time access decisions. ML is used to assist decision making based on advanced network analytics (full packet capture, etc.). Policies are consistently implemented across the enterprise using unified access standards.	Analyze SIEM logs with analytics engine to provide real-time policy access decisions; Support sending captured packets, data/network flows, and other specific logs for analytics; Segment end-to-end transport network flows; Audit security policies for consistency across enterprise; Protect data in transit during coalition information sharing
5.3.1	Data Center Macrosegmentation	DoD organizations implement data center-focused macrosegmentation using traditional tiered (web, app, db) and/or service-based architectures. Proxy and/or enforcement checks are integrated with the SDN solution(s) based on device attributes and behavior.	Log actions to SIEM; Establish proxy/enforcement checks of device attributes, behavior, and other data; Analyze activities with analytics engine
5.3.2	B/C/P/S Macrosegmentation	DoD organizations implement base, camp, post, and station macrosegmentation using logical network zones limiting lateral movement. Proxy and/or enforcement checks are integrated with the SDN solution(s) based on device attributes and behavior.	Establish proxy/enforcement checks of device attributes, behavior, and other data; Log actions to SIEM; Analyze activities with analytics engine; Leverage SOAR to provide real-time policy access decisions

Pillar 5: Network & Environment–Activities

ID	Activity Name	Description	Outcomes
5.4.1	Implement Microsegmentation	DoD organizations implement microsegmentation infrastructure into SDN environment, enabling basic segmentation of service components (e.g., web, app, db), ports, and protocols. Basic automation is accepted for policy changes, including API decision making. Virtual hosting environments implement microsegmentation at the host/container level.	Accept automated policy changes; Implement API decision points; Implement NGF/Micro FW/Endpoint Agent in virtual hosting environment
5.4.2	Application & Device Microsegmentation	DoD organizations utilize SDN solution(s) to establish infrastructure meeting the ZT target functionalities: logical network zones-, role-, attribute-, and conditional-based access control for user and devices, PAM services for network resources, and policy-based control on API access.	Assign role-, attribute-, and condition-based access control to user and devices; Provide PAM services; Limit access on per-identity basis for user and device; Create logical network zones; Support policy control via REST API
5.4.3	Process Microsegmentation	DoD organizations utilize existing microsegmentation and SDN automation infrastructure, enabling process microsegmentation. Host-level processes are segmented based on security policies and access is granted using real-time access decision making.	Segment host-level processes for security policies; Support real-time access decisions and policy changes; Support offload of logs for analytics and automation; support dynamic deployment of segmentation policy
5.4.4	Protect Data In Transit	Based on the data flow mappings and monitoring, policies are enabled by DoD organizations to mandate protection of data in transit. Common use cases, such as coalition information sharing, sharing across system boundaries, and protection across architectural components, are included in protection policies.	Protect data in transit during coalition information sharing; Protect data in transit across system high boundaries; Integrate data in transit protection across architecture components

Pillar 6: Automation & Orchestration

Capability	Capability Description	Impact to ZT	Associated Activities	Juniper Products/Solutions
6.1 Policy Decision Point (PDP) & Policy Orchestration	DoD organizations initially collect and document all rule-based policies to orchestrate across the security stack for effective automation. DAAS access procedures and policies will be defined, implemented, and updated. Organizations mature this capability by establishing PDPs and PEPs (including the Next-Generation Firewall) to make DAAS resource determinations and enable, monitor, and terminate connections between a user/device and DAAS resources according to predefined policy.	PDPs and PEPs ensure proper implementation of DAAS access policies to users or endpoints that are properly connected (or denied access) to requested resources	*Policy Inventory & Development *Organization Access Profile *Enterprise Security Profile Pt. 1 *Enterprise Security Profile Pt. 2	N/A
6.2 Critical Process Automation	DoD organizations employ automation methods such as RPA to address repetitive, predictable tasks for critical functions such as data enrichment, security controls, and incident response workflows according to system security engineering principles.	Response time and capability is increased with orchestrated workflows and risk management processes	*Task Automation Analysis *Enterprise Integration & Workflow Provisioning Pt. 1 *Enterprise Integration & Workflow Provisioning Pt. 2	Juniper Networks has intent-based control point software for Day 0-1-2. The control point software is specific to the product sets we build for: WAN, DC, campus and branch, and security use cases. The Paragon Network Automation Platform and products powered by AI and ML are designed to provide end users with an assured service experience. Paragon Active Assurance is a programmable, active test and monitoring solution for physical, hybrid, and virtual networks that verifies application and service performance. Paragon Insights is a network health and diagnostic solution that provides operational intelligence across all service provider, cloud, and enterprise network domains, from network access to servers in the data center. Paragon Network Trust and Compliance provides automated, consistent, and reliable network trust and compliance that can verify, confirm, and quantify the trust aspects of the network, making it easier for network operators to run trustworthy networks. The cloud-based automation solution measures the risk of integrity impairment and trust posture of network infrastructure. In parallel, it provides insight and nonintrusive validation of trustworthiness and reliability throughout the network.
6.3 Machine Learning	DoD organizations employ ML to execute (and enhance the execution of) critical functions such as incident response, anomaly detection, user baselining, and data tagging.	Response time and capability is increased with orchestrated workflows and risk management processes	*Implement Data Tagging & Classification ML Tools	Recent advances in generative AI catapulted AI and ML into the corporate, federal, service provider, and cloud provider spotlight. Data centers are the engines behind AI, and data center networks play a critical role in interconnecting and maximizing the utilization of costly GPU servers. AI training, measured by job completion time (JCT), is a massive parallel processing problem. A fast and reliable network fabric is needed to get the most out of your expensive GPUs. The right network is key to optimizing ROI and the formula is simple: design the right network, save big on AI applications.

Pillar 6: Automation & Orchestration

Capability	Capability Description	Impact to ZT	Associated Activities	Juniper Products/Solutions
6.4 Artificial Intelligence	DoD organizations employ AI to execute (and enhance the execution of) critical functions, particularly risk and access determinations and environmental analysis.	Response time and capability is increased with orchestrated workflows and risk management processes	*Implement AI Automation Tools *AI Driven by Analytics Decides A&O Modifications	Recent advances in generative AI catapulted AI and ML into the corporate, federal, service provider and cloud provider spotlight. Data centers are the engines behind AI, and data center networks play a critical role in interconnecting and maximizing the utilization of costly GPU servers. AI training, measured by job completion time (JCT), is a massive parallel processing problem. A fast and reliable network fabric is needed to get the most out of your expensive GPUs. The right network is key to optimizing ROI and the formula is simple: design the right network, save big on AI applications.
6.5 Security Orchestration, Automation, & Response (SOAR)	DoD organizations achieve initial operational capability of security technologies to orchestrate and automate policies (e.g., PEPs and PDPs) and rulesets to improve security operations, threat and vulnerability management, and security incident response by ingesting alert data, triggering playbooks for automated response and remediation.	Pre-defined playbooks, from collection to incident response and triage, enable initial process automation that accelerates a security team's decision and response speed	*Response Automation Analysis *Implement SOAR Tools *Implement Playbooks	Juniper's Security Director software offers centralized security policy management, automation, and response across physical, virtual, and containerized firewalls. Install on-prem and operate through a modern and centralized web-based interface.
6.6 API Standardization	DoD establishes and enforces enterprise-wide programmatic interface (e.g., API) standards. All non-compliant APIs are identified and replaced.	Standardizing APIs across the department improves application interfaces, enabling orchestration and enhancing interoperability	*Tool Compliance Analysis *Standardized API Calls & Schemas Pt. 1 *Standardized API Calls & Schemas Pt. 2	Juniper Networks uses standardized applications programming interfaces across all products and control point software. Examples include: Paragon Pathfinder API Documentation, Threat Intelligence Open API, and Junos OS REST API Guide.
6.7 Security Operations Center (SOC) & Incident Response (IR)	In the event a computer network defense service provider (CNDSP) does not exist, DoD organizations define and stand up SOC to deploy, operate, and maintain security monitoring, protections, and response for DAAS. SOCs provide security management visibility for status (upward visibility) and tactical implementation (downward visibility). Workflows within the SOC are automated using automation tooling and enrichment occurs between service providers and technologies.	Standardized, coordinated, and accelerated incident response and investigative efforts	*Workflow Enrichment Pt. 1 *Workflow Enrichment Pt. 2 *Workflow Enrichment Pt. 3 *Automated Workflow	N/A

Pillar 6: Automation & Orchestration–Activities

ID	Activity Name	Outcomes
6.1.1	Policy Inventory & Development	Policies have been collected in reference to applicable compliance and risk (e.g. RMF, NIST); Policies have been reviewed for missing pillars and capabilities per the ZTRA; Missing areas of policies are updated to meet the capabilities per ZTRA
6.1.2	Organization Access Profile	Organization scoped profile(s) are created to determine access to DAAS using capabilities from user, data, network, and device pillars; Initial enterprise profile access standard is developed for access to DAAS; When possible, the organization profile(s) utilizes enterprise available services in the user, data, network, and device pillars; Organization mission/task-critical profile(s) are created
6.1.3	Enterprise Security Profile Pt. 1	Enterprise profile(s) are created to access DAAS using capabilities from user, data, network, and device pillars; Non-mission/task critical organization profile(s) are integrated with the enterprise profile(s) using a standardized approach
6.1.4	Enterprise Security Profile Pt. 2	Enterprise profile(s) have been reduced and simplified to support widest array of access to DAAS; Where appropriate, mission/task-critical profile(s) have been integrated and supported organization profiles are considered the exception
6.2.1	Task Automation Analysis	Automatable tasks are identified; Tasks are enumerated
6.2.2	Enterprise Integration & Workflow Provisioning Pt. 1	Implement full enterprise integration; Identify key integrations; Identify recovery and protection requirements
6.2.3	Enterprise Integration & Workflow Provisioning Pt. 2	Services identified; Service provisioning is implemented
6.3.1	Implement Data Tagging & Classification ML Tools	Implemented data tagging and classification tools are integrated with ML tools
6.4.1	Implement AI Automation Tools	Develop AI tool requirements; Procure and implement AI tools
6.4.2	AI Driven by Analytics Decides A&O Modifications	AI is able to make changes to automated workflow activities
6.5.1	Response Automation Analysis	Automatable response activities are identified; Response activities are enumerated
6.5.2	Implement SOAR Tools	Develop requirements for SOAR tool; Procure SOAR tools
6.5.3	Implement Playbooks	When possible, automated playbooks based on automated workflows capability; Manual playbooks are developed and implemented
6.6.1	Tool Compliance Analysis	API status is determined compliance or non-compliance to API standards; Tools to be used are identified
6.6.2	Standardized API Calls & Schemas Pt. 1	Initial calls and schemas are implemented; Non-compliant tools are replaced
6.6.3	Standardized API Calls & Schemas Pt. 2	All calls and schemas are implemented
6.7.1	Workflow Enrichment Pt. 1	Threat events are identified; Workflows for threat events are developed
6.7.2	Workflow Enrichment Pt. 2	Workflows for advanced threat events are developed; Advanced threat events are identified
6.7.3	Workflow Enrichment Pt. 3	Enrichment data has been identified; Enrichment data is integrated into workflows
6.7.4	Automated Workflow	Workflow processes are fully automated; Manual processes have been identified; Remaining processes are marked as exceptions and documented

Pillar 7: Visibility and Analytics

Capability	Capability Description	Capability Outcome	Impact to ZT	Associated Activities	Juniper Products/Solutions
7.1 Log All Traffic (Network, Data, Apps, Users)	DoD organizations collect and process all logs, including network, data, application, device, and user logs and make those logs available to the appropriate Computer Network Defense Service Provider (CNDSP) or security operations center (SOC). Logs and events follow a standardized format and rules/analytics are developed as needed.	DoD organizations collect and process all logs, including network, data, application, device, and user logs and make those logs available to the appropriate Computer Network Defense Service Provider (CNDSP) or security operations center (SOC).	Foundational to the development of automated hunt and incident response playbooks	*Scale Considerations *Log Parsing *Log Analysis	Security Director Cloud provides for the ingestion, parsing, storage, retrieval, and presentation of syslog event logs, including device component-level information, AAA RBAC and command execution, policy and config changes, session logs, user firewall (AD) policies, L7 application identification and usage by user/session count/BW, malware, and threats. Virtually unlimited scale is made possible by cloud storage. The Juniper Secure Analytics SIEM Virtual Appliance "All-in-One" runs all core functions on the same physical hardware and can process up to 30,000 events per second (EPS) and 1,200,000 flows per minute (FPM) while the **JSA Virtual Appliance Distributed** supports up to 80,000 EPS and 3,600,000 FPM, depending on the VM specifications.
7.2 Security Information and Event Management (SIEM)	CNDSP or SOC monitor, detect, and analyze data logged into a security information and event management (SIEM) tool. User and device baselines are created using security controls and integrated with the SIEM. Alerting within the SIEM is matured over the phases to support more advanced data points (e.g., Cyber Threat Intel, Baselines).	CNDSPs/SOCs monitor, detect, and analyze data logged into an SIEM tool.	Processing and exploiting data in the SIEM enables effective security analysis of anomalous user behavior, alerting, and automation of relevant incident response to common threat events	*Threat Alerting Pt. 1 *Threat Alerting Pt. 2 *Threat Alerting Pt. 3 *Asset ID & Alert Correlation *User/Device Baselines	The JSA Series Secure Analytics Virtual Appliance is an SIEM system specifically designed for virtualized IT and cloud environments. It collects and consolidates security events from thousands of network devices, computing endpoints, and applications across your distributed infrastructure. Using big data analytics, it provides you with an actionable list of offenses that accelerates incident remediation and improves your digital security. Reporting and alerting capabilities for control framework: • Control Objectives for Information and related Technology (CobiT) • International Organization for Standardization (ISO) ISO/IEC 27002 (17799) • Common Criteria (CC) (ISO/IEC 15408) NIST special publication 800-53 revision 1 and Federal Information Processing • Standard (FIPS) 20
7.3 Common Security & Risk Analytics	CNDSPs or SOCs employ data tools across their enterprises for multiple data types to unify data collection and examine events, activities, and behaviors.	CNDSPs/SOCs employ big data tools across their enterprises for multiple data types to unify data collection and examine events, activities, and behaviors.	Analysis integrated across multiple data types to examine events, activities, and behaviors	*Implement Analytics Tools *Establish User Baseline Behavior	JSA Series Secure Analytics takes an innovative approach to managing computer-based threats in the enterprise. Recognizing that discrete analysis of security events is not enough to properly detect threats, we developed the JSA Series Secure Analytics to provide an integrated approach to threat analytics that combines the use of traditionally siloed information to more effectively detect and manage today's complex threats. Specific information that is collected includes: Network Events, Security Logs, Host and Application Logs, Network and Application Flow Logs, User and Asset Identity Information, and Protocol (LDAP).

Pillar 7: Visibility and Analytics

Capability	Capability Description	Capability Outcome	Impact to ZT	Associated Activities	Juniper Products/Solutions
7.4 User & Entity Behavior Analytics	DoD organizations initially employ analytics to profile and baseline activity of users and entities and to correlate user activities and behaviors and detect anomalies. CNDSPs or SOCs mature this capability through the employment of advanced analytics to profile and baseline activity of users and entities, correlate user activities and behaviors, and detect anomalies.	DoD organizations initially employ analytics to profile and baseline activity of users and entities, correlate user activities and behaviors, and detect anomalies. CNDSPs/ SOCs mature this capability through the employment of advanced analytics to profile and baseline activity of users and entities, correlate user activities and behaviors, and detect anomalies.	Advanced analytics support detection of anomalous users, devices, and NPE actions and advanced threats	*Baseline & Profiling Pt. 1 *Baseline & Profiling Pt. 2 *UEBA Baseline Support Pt. 1 *UEBA Baseline Support Pt. 2	Juniper Secure Analytics Virtual Appliance has User Behavior Analytics rules that can help you identify potential insider threats in your network. Then, the data automatically displays in the QRadar User Behavior Analytics dashboards so you can visualize the risks to your network.
7.5 Threat Intelligence Integration	CNDSPs or SOCs integrate threat intelligence information and streams about identities; motivations; characteristics; and tactics, techniques, and procedures (TTPs) with data collected in the SIEM.	CNDSPs or SOCs integrate threat intelligence information and streams about identities; motivations; characteristics; and tactics, techniques, and procedures (TTPs) with data collected in the SIEM.	Integrating threat intelligence into other SIEM data enhances monitoring efforts and incident response	*Cyber Threat Intelligence Program Pt. 1 *Cyber Threat Intelligence Program Pt. 2	**Juniper Networks X-Force** security experts use a series of international data centers to collect tens of thousands of malware samples, analyze web pages and URLs, and run analysis to categorize potentially malicious IP addresses and URLs. X-Force Exchange is the platform for sharing this data, which can be used in JSA. Juniper ATP SecIntel feeds provide carefully curated and verified threat intelligence from Juniper Networks' Advanced Threat Prevention (ATP) Cloud, Juniper Threat Labs, Dynamic Address Group (DAG), and industry-leading threat feeds to MX Series routers, SRX Series Firewalls, and NFX Series Network Services Platform to block Command and Control (C&C) communications at line rate. SecIntel delivers real-time threat intelligence by enabling automatic and responsive traffic filtering.
7.6 Automated Dynamic Policies	DoD organization AI/ML solutions dynamically and automatically update security profiles and device configuration through continuous security posture monitoring, risk and confidence scoring, and automated patch management.	CNDSPs/SOCs dynamically and automatically update security profiles and device configuration through continuous security posture monitoring, risk and confidence scoring, and automated patch management.	Users and NPEs are denied access based on automated, real-time security profiles based on external conditions and evolving risk and confidence scores	*AI-Enabled Network Access *AI-Enabled Dynamic Access Control	Juniper ATP Cloud Adaptive Threat Profiling allows SRX Series Firewalls to generate, propagate, and consume threat feeds based on their own advanced detection and policy-match events. This feature allows you to configure security or IDP policies that, when matched, inject the source IP address, destination IP address, source identity, or destination identity into a threat feed, which can be leveraged by other devices as a dynamic-address-group (DAG). While this feature is focused on tracking and mitigating threat actors within a network, you can also use it for non-threat related activities, such as device classification. With adaptive threat profiling, the Juniper ATP Cloud service acts as a feed-aggregator and consolidates feeds from SRX across your enterprise and shares the deduplicated results back to all SRX Series Firewalls in the realm at regular intervals. SRX Series Firewalls can then use these feeds to perform further actions against the traffic.

Pillar 7: Visibility and Analytics–Activities

ID	Activity Name	Outcomes	Juniper Products/Solutions
7.1.1	Scale Considerations	Sufficient infrastructure in place; Distributed environment established; Sufficient bandwidth for network traffic	Juniper's central management portal, Security Director Cloud, operates in AWS, providing ultimate resiliency and scale. The Juniper Secure Analytics SIEM Virtual Appliance “All-in-One” runs all core functions on the same physical hardware and can process up to 30,000 events per second (EPS) and 1,200,000 flows per minute (FPM) while the JSA Virtual Appliance Distributed supports up to 80,000 EPS and 3,600,000 FPM, depending on the VM specifications.
7.1.2	Log Parsing	Standardized log formats; Rules developed for each log format	SRX on-box traffic logging to solid-state drives (SSDs) supports eight external log servers or files. An all-in-one XML file is added that contains all the traffic logs information. The XML file also generates all the logging header files and traffic log related documents. A process (daemon) called local log management daemon (llmd) saves these logs to the local SSD. Traffic logs are saved in the five different formats: syslog, sd-syslog, WELF, Binary, and protobuf (Google). In addition, Juniper Secure Analytics SIEM supports the Lof Event Extended Format (LEEF). The LEEF is a customized event format for JSA that contains readable and easily processed events for JSA. The LEEF format consists of a syslog header, a LEEF header, and event attributes.
7.1.3	Log Analysis	Develop analytics per activity; Identify activities to analyze	Security Director Insights empowers organizations to automate threat remediation and microsegmentation policies across the entire network with Security Director’s built-in orchestration. Security Director Insights collects and automatically correlates data across multiple security layers—email, endpoint, server, cloud workloads, and network—so threats are detected faster and security teams can improve investigation and response times. It also uses mitigation rules to prevent future attacks. With Security Director Insights, customers can: • Understand when and where an attack is happening by using it to correlate and prioritize security events from multiple security solutions across various parts of the network • Use custom threat and incident scoring so that security teams can respond to and mitigate attacks that have the potential to do the most harm to the business • Mitigate active threats across the network—on Juniper SRX Series firewalls—with one click
7.2.1	Threat Alerting Pt. 1	Rules developed for threat correlation	Security Director Insights expands end-to-end visibility by correlating and scoring threat events across the complete security stack. It offers a timeline view mapped to the MITRE attack framework so administrators can focus on the highest-priority threats. It unifies visibility across the network by correlating threat detection information, including detections from other vendor products, and enables one-touch mitigation to address gaps in defense quickly. Security Director Insights empowers organizations to automate threat remediation and microsegmentation policies across the entire network with Security Director’s built-in orchestration.
7.2.2	Threat Alerting Pt. 2	Develop analytics to detect deviations	Customers can use Security Director Insights to track attack indicators across their networks, from client to workload, regardless of which vendor product in their environment made the detection. In Security Director, Policy Enforcer provides simplified user intent-based threat management policy modification and distribution tool.
7.2.3	Threat Alerting Pt. 3	Identify triggering anomalous events; Implement triggering policy	Juniper Secure Analytics Virtual Appliance has User Behavior Analytics rules that can help you identify potential insider threats inside your network. Then, the data automatically displays in the QRadar User Behavior Analytics dashboards so that you can visualize the risks to your network. From login failure attempts to remote procedure calls across network segements, JSA tracks user behavior and triggers built-in and custom "offenses."
7.2.4	Asset ID & Alert Correlation	Rules developed for asset ID-based responses	Juniper Secure Analytics provides extensibility to extract values from event logs to create custom rules and alerts. Device ID, type, manufacturer, and S/N are examples.

Pillar 7: Visibility and Analytics–Activities

ID	Activity Name	Outcomes
7.2.5	User/Device Baselines	Identify user and device baselines
7.3.1	Implement Analytics Tools	Develop requirements for analytic environment; Procure and implement analytic tools
7.3.2	Establish User Baseline Behavior	Identify users for baseline; Establish ML-based baselines
7.4.1	Baseline & Profiling Pt.1	Develop analytics to detect changing threat conditions; Identify user and device threat profiles
7.4.2	Baseline & Profiling Pt. 2	Add threat profiles for IoT and OT devices; Develop and extend analytics; Extend threat profiles to individual users and devices
7.4.3	UEBA Baseline Support Pt. 1	Implement ML-based analytics to detect anomalies
7.4.4	UEBA Baseline Support Pt. 2	Implement ML-based analytics to detect anomalies
7.5.1	Cyber Threat Intelligence Program Pt. 1	CTI team is in place with critical stakeholders; Public and Baseline CTI feeds are being utilized by SIEM for alerting; Basic integration points exist with Device and Network enforcement points (e.g., NGAV, NGFW, and NG-IPS)
7.5.2	Cyber Threat Intelligence Program Pt. 2	CTI team is in place with extended stakeholders as appropriate; Controlled and Private feed are being utilized by SIEM and other appropriate analytics tools for alerting and monitoring; Integration is in place for extended enforcement points within the Device, User, Network, and Data pillars (UEBA and UAM)
7.6.1	AI-Enabled Network Access	Network access is AI driven based on environment analytics
7.6.2	AI-Enabled Dynamic Access Control	JIT/JEA are integrated with AI; Access is AI driven based on environment analytics

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

7400191-001-EN July 2024