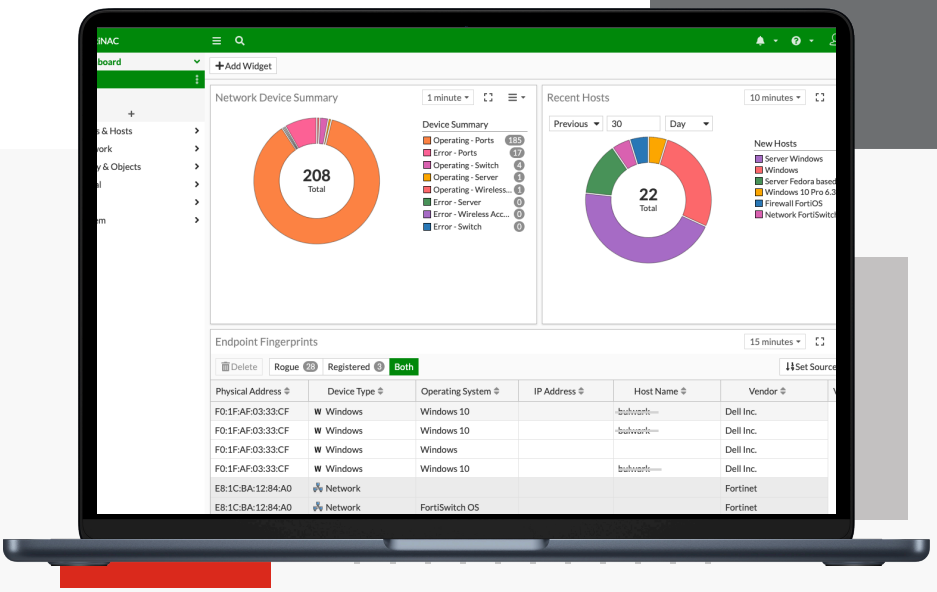
FortiNAC

FortiNAC F Series Hardware, VM, and Endpoint Licenses



Highlights

- Implement dynamic network scanning to classify and analyze device behaviors using continuous, automated techniques
- Maintain an updated inventory of all network devices, including BYOD, IoT, OT, and IoMT
- Continuously assess risks for every endpoint using real-time threat intelligence and behavioral patterns
- Adopt Zero Trust architecture for better device security and simplified management
- Integrate with various third-party network tools ensuring compatibility
- Relay real-time contextual data to SIEM, improving incident response. Ensure always-on identity checks and follow least privilege access, reinforcing the Zero Trust approach

Visibility, Zero Trust Access and Incident Response for Connected Assets and Users

FortiNAC™ continues to be a cutting-edge network access control solution, enabling organizations to enforce network access policies and assure adherence to security protocols in light of increasingly sophisticated threats. It provides a comprehensive snapshot of all devices and users on the network, facilitating granular control of access based on user roles, device types, network locations, and now the behavioral patterns of devices and users.

The solution's capability now extends beyond automated onboarding of new endpoints; it incorporates real-time threat intelligence and continuous risk assessment of devices, leveraging machine learning and AI technologies from FortiGuard Services. Given the rising prominence of BYOD (Bring Your Own Device) and IoT (Internet of Things), FortiNAC's continuous monitoring and immediate remediation of non-compliant devices have become even more crucial.

Moreover, FortiNAC's integration goes beyond third-party security solutions; it integrates with a wide range of cloud-based platforms and DevOps tools to ensure seamless and secure network operations in hybrid IT environments. FortiNAC leverages its integration with FortiAnalyzer to gain deep insight into network security posture, encompassing real-time visibility, predictive analytics, and more robust compliance reporting. With FortiNAC, organizations can more effectively secure their network against unauthorized access, potential threats, and increasingly, the insider threats, aligning with the emerging Zero Trust security model that emphasizes "never trust, always verify".

Available in

Appliance

Virtual

Features

Granular Visibility Across the Network for Every Device and User

FortiNAC leverages AI and machine learning from FortiGuard Security Services to provide detailed profiling of devices, including headless devices and IoT assets on your network. This profiling incorporates multiple information sources, behavior patterns, and real-time threat intelligence to accurately identify and assess what is on your network.

Seamless Integration and Control Across Diverse Environments

With the power of micro-segmentation and Zero Trust policies, FortiNAC allows for configuration changes on switches and wireless products from an extended range of vendors. It amplifies the reach of the Security Fabric across multi-cloud, hybrid IT, and heterogeneous environments, implementing “never trust, always verify’ principles.

Automated Responsiveness

FortiNAC reacts to network events in real-time to contain threats before they spread, utilizing a broad and customizable set of automation policies. Leveraging AI, these policies can instantly trigger configuration changes and remediation actions when targeted behavior or anomalies are observed, aligning with the Zero Trust model’s dynamic and proactive approach.

New FortiNAC-F

FortiNAC introduces the new FortiNAC-F OS with hardened virtual and physical appliances that increase security and compliance capabilities. Following the tradition of providing the reliable platforms of Fortinet, the new FortiNAC-F will extend the performance capability and introduce new features.

FortiNAC 21 Profiling Methods for Device Classification

Highlights

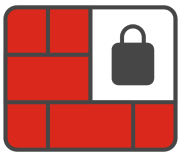
Granular Device Visibility

The essence of securing a dynamic, ever-evolving network lies in comprehending its makeup. FortiNAC leverages AI and machine learning from FortiGuard Security Services, goes beyond merely “seeing” everything on the network—it comprehends and analyzes. It scans your network to discover every user, application, and device. Using a variety of techniques—it profiles each element based on observed behavior, real-time threat intelligence, as well as tapping into FortiGuard’s IoT Services, a cloud-based database for identification lookups.

Scanning can be active or passive, utilizing permanent agents, dissolvable agents, or agentless approaches. Moreover, FortiNAC can evaluate a device against pre-approved profiles, noting any discrepancies or software updates required to patch vulnerabilities. With FortiNAC, the network isn’t just known—it’s understood, assessed, and continually monitored.

Besides recognizing the entire network, FortiNAC’s advanced visibility incorporates passive traffic analysis, leveraging Fortinet FortiGate appliances as sensors to identify anomalous behavior patterns. These patterns can indicate a potential compromise, triggering real-time alerts for the SOC team and aligning with the proactive threat containment approach integral to the Zero Trust model.

Highlights



Network Security and Intelligent Segmentation

After successful classification of devices and user identification, FortiNAC now integrates advanced segmentation techniques to ensure only authorized users and devices have access to requisite resources, thus preventing unauthorized intrusion. Through its progressive role-based network access control, FortiNAC allows for strategic network segmentation by logically grouping similar data and applications, limiting access to a particular set of users or devices. This strategy effectively confines a compromised device, thereby inhibiting its ability to traverse the network and inflict damage on other resources. FortiNAC not only fortifies the protection of sensitive data and vital assets but also ensures adherence to internal, industrial, and government regulations and mandates.

Device Integrity Verification and Malware Prevention

FortiNAC emphasizes on the importance of device integrity prior to network connection, significantly reducing the risk and potential spread of malicious software. As a device attempts to join the network, FortiNAC assesses its configuration for compliance. Any non-compliant configuration is promptly managed; for instance, the device may be allocated to an isolated or restricted access VLAN, devoid of any access to corporate resources. This feature has become increasingly relevant with the rise of IoT devices and remote work trends, ensuring a secure and controlled network environment.

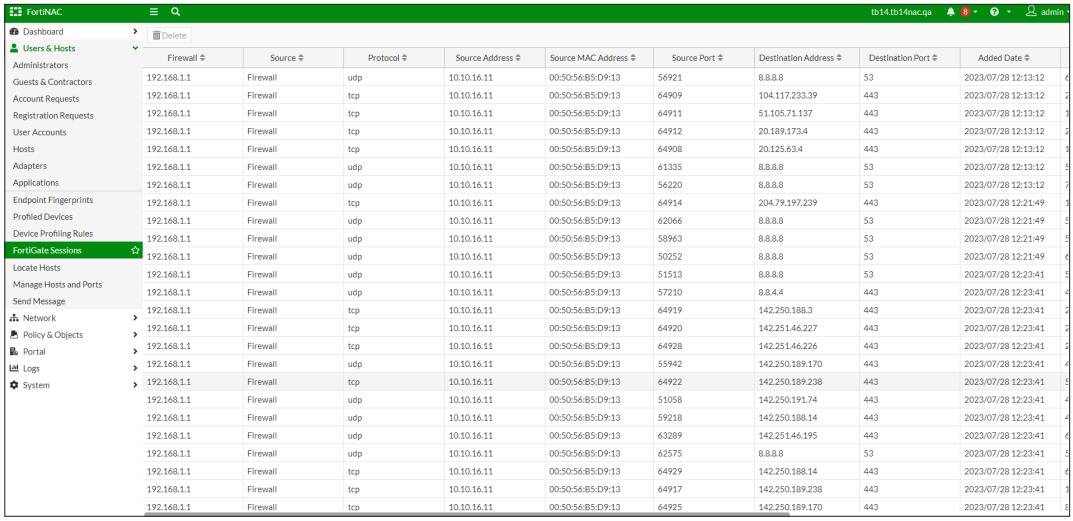
Intelligent Monitoring and Automated Reaction

FortiNAC proactively supervises the network continuously, examining endpoints to verify their compliance with predefined profiles. Leveraging modern security tactics, FortiNAC rescreens devices to prevent any possible bypassing of network access security via MAC-address spoofing. Further, FortiNAC is equipped to identify irregularities in traffic patterns, a vital feature considering the growing complexities in network usage patterns with the rise of cloud and edge computing. This passive anomaly detection function operates symbiotically with FortiGate appliances. Upon recognizing a compromised or susceptible endpoint as a potential risk, FortiNAC promptly instigates an automated reaction, quarantining the endpoint in real-time, furthering its commitment to maintaining a secure and controlled network environment.

Highlights

FortiGate Sessions View

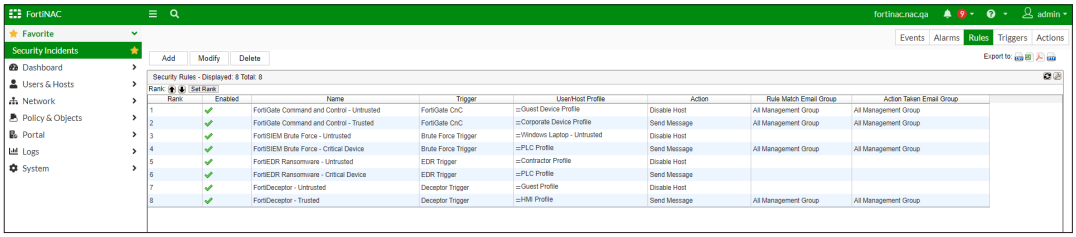
The FortiGate Sessions view adds the ability to accept netflow data from third party devices. Flows from other devices would also show up in this view.



FortiNAC 21 Profiling Methods for Device Classification

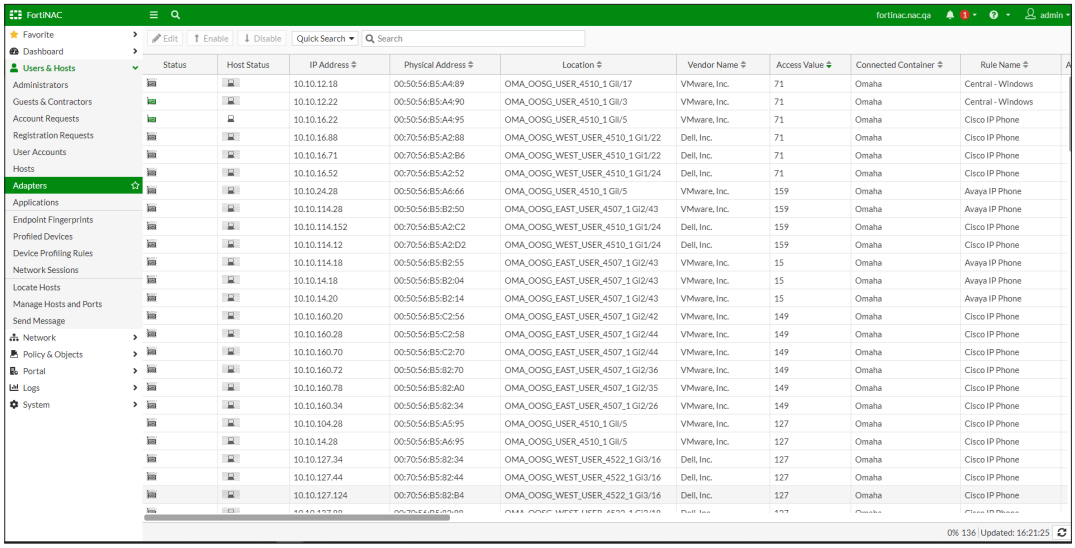
Security Fabric Integrations

FortiNAC integrates with multiple Fortinet products such as FortiGate, FortiSIEM, FortiAnalyzer, FortiEDR, and FortiDeceptor. The Security Rules are triggered by syslog/snmp messages from the other Fortinet products as shown below.

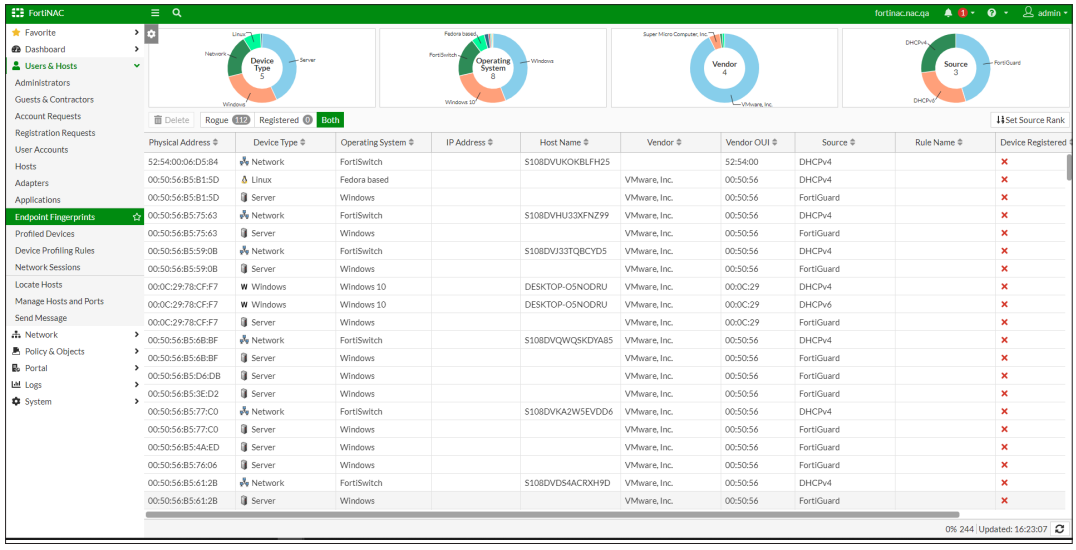


FortiNAC Security Rules

Integration



FortiNAC Adapter View



FortiNAC New Endpoint Fingerprints View

Integration

Extensive integration with desktop security software, directories, network infrastructure, and third-party security systems provides unparalleled visibility and control across the network environment.

The FortiNAC family integrates

- More than 3000 devices with unique MIB OIDs
- More than 2000 models including switches, access points, and network controllers
- More than 90 vendors in networking, security, and communication industries

with the following vendor and models as examples*.

Network Infrastructure	Adtran, Aerohive, AlaxalA Networks, Alcatel-Lucent, Allied Telesis, Alteon, APC, Apple, APRESIA Systems, Avaya, Brocade/Foundry Networks/Ruckus, Cisco/Meraki, D-Link, Extreme/Enterasys/Siemens, H3C, HP/Colubris/3Com/Aruba, Intel, Juniper, NEC, Riverbed/Xirrus, and SonicWall
Security Infrastructure	CheckPoint, Cisco/SourceFire, Cyphort, FireEye, Juniper/ Netscreen, Qualys, Sonicwall, Tenable
Authentication and Directory Services	RADIUS — Cisco ACS, Free RADIUS, Microsoft IAS, LDAP — Google SSO, Microsoft Active Directory, OpenLDAP
Operating Systems	Android, Apple MAC OSX and iOS, Linux, Microsoft Windows
Endpoint Security Applications	Authentium, Avast, AVG, Avira, Blink, Bullguard, CA, ClamAV, Dr. Web, Enigma, ESET, F-Prot, F-Secure, G Data, Intego, Javacool, Lavasoft, Lightspeed, McAfee, Microsoft, MicroWorld, Norman, Norton, Panda, PC Tools, Rising, Softwin, Sophos, Spyware Bot, Sunbelt, Symantec, Trend Micro, Vexira, Webroot SpySweeper, Zone Alarm
Mobile Device Management	AirWatch, Google GSuite, MaaS360, Microsoft InTune, Mobile Iron, XenMobile, JAMF, Nozomi Networks

* FortiNAC can be integrated with other vendors and technologies in addition to those listed here. This list represents integrations that have been validated in both test lab and production network environments.

Deployment Options

Easy Deployment

FortiNAC is a flexible and scalable solution that spans from mid-size to very large enterprise deployments. There are three elements to the FortiNAC solution.

- Application and Control (required)
- Management (optional)
- FortiAnalyzer for Reports (optional)

The Application provides the visibility, and the Control provides the configuration capabilities and automated responsiveness features. The Management portion enables the sharing of concurrent users across a multi-server deployment. FortiAnalyzer provides reports and analytics based on the information gathered from the network through FortiNAC.

FortiNAC can be deployed in virtual machines (VMWare/Hyper-V/ AWS/ Azure/ KVM) or on hardware appliances. The Application and Control Servers can be deployed in a variety of sizes, depending on the number of ports they need to support. FortiNAC is ideal for support distributed architectures, including SD-Branch locations.

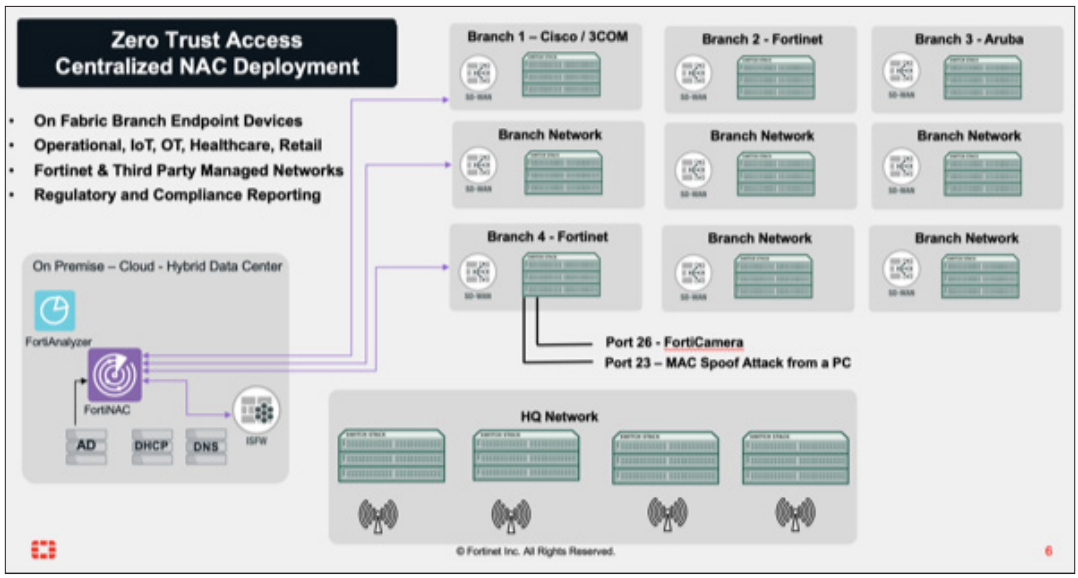
High Availability

FortiNAC offers High Availability for disaster recovery to ensure redundancy. This state is achieved through active and passive instances where the passive (backup) becomes active when the main is no longer functioning normally. FortiNAC Manager can manage multiple high availability clusters distributed throughout the network as needed.

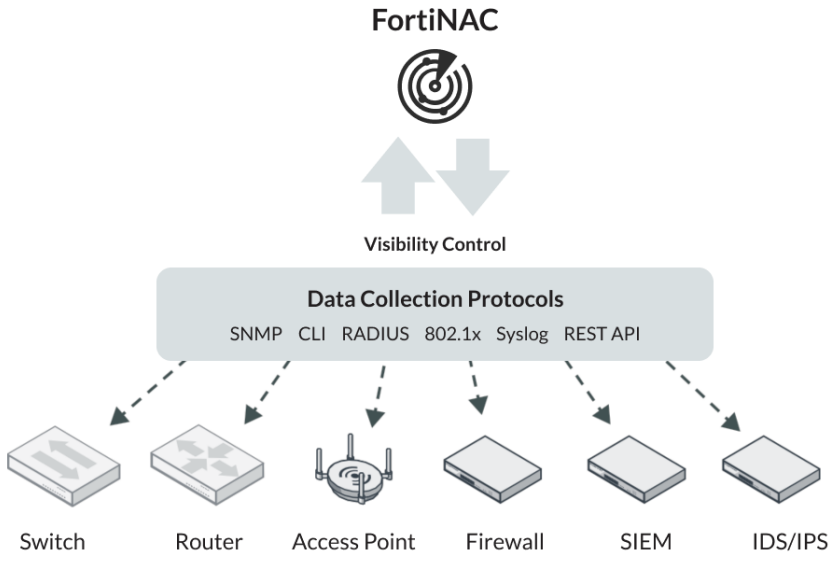
Deployment Options

Centralized Architecture

FortiNAC is an 'out of band' solution, meaning it does not sit in-line of user traffic. This architecture allows FortiNAC to be deployed centrally and manage many remote locations. Visibility, control, and response are achieved by integrating with, and leveraging the capabilities of, the network infrastructure. Control can be applied at the point of connection, at the very edge of the network while security device integrations allow FortiNAC to process security alerts and treat them as triggers for automated threat mitigation through customizable work flows.



Data collection is gathered from multiple sources using a variety of methods. SNMP, CLI, RADIUS, SYSLOG, API and DHCP fingerprints can all be used to achieve the detailed end-to-end visibility necessary to create a truly secure environment.



Licensing

FortiNAC Licensing

FortiNAC offers flexible deployment options based on the level of coverage and functionality desired.

Base License

The BASE license level provides easy, one-step IoT security solution to close pressing endpoint security gaps by seeing all endpoint devices on the network, automating authorization, and enabling micro-segmentation and network lockdown. The BASE license level is appropriate for organizations that need to secure IoT and headless devices, and enable network lockdown with dynamic VLAN steering, but do not require more advanced user/network controls or automated threat response.

Plus License

The PLUS license level builds on all the functionality of BASE with enhanced visibility and more advanced Network Access Controls and automated provisioning for users, guests, and devices as well as reporting and analytics. The reporting and analytics can greatly assist in providing audit documentation of compliance. The PLUS license level is appropriate for organizations that want complete endpoint visibility and a granular control, but do not require automated threat response.

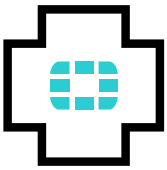
Pro License

The PRO license level provides the ultimate in visibility, control and response. PRO license offers real-time endpoint visibility, comprehensive access control, and automated threat response and delivers contextual information with triaged alerts. The PRO license level is appropriate for organizations that want complete endpoint visibility, a flexible NAC solution with granular controls, as well as accurate event triage and real-time automated threat response.

Licensing

		FORTINAC LICENSE TYPES	BASE	PLUS	PRO
Visibility	Network	Network Discovery	✓	✓	✓
		Rogue Identification	✓	✓	✓
		Device Profiling and Classification	✓	✓	✓
	Endpoint	Enhanced Visiblity	✓	✓	✓
		Anomaly Detection	✓	✓	✓
		MDM Integration	✓	✓	✓
		Persistent Agent	✓	✓	✓
	User	Authentication		✓	✓
		Captive Portal		✓	✓
Automation / Control		Network Access Policies	✓	✓	✓
		IoT Onboarding with Sponsor	✓	✓	✓
		Rogue Device Detection and Restriction	✓	✓	✓
		Firewall Segmentation	✓	✓	✓
		MAC Address Bypass (MAB)	✓	✓	✓
		Full RADIUS (EAP)	✓	✓	✓
		BYOD / Onboarding		✓	✓
		Guest Management		✓	✓
		Endpoint Compliance		✓	✓
		Web and Firewall Single Sign-on	✓	✓	✓
Incident Response		Event Correlation			✓
		Extensible Actions and Audit Trail			✓
		Alert Criticality and Routing			✓
		Guided Triage Workflows			✓
Integrations		Inbound Security Events			✓
		Outbound Security Events	✓	✓	✓
		REST API	✓	✓	✓
Reporting		Customizable Reports	✓	✓	✓

Services



FortiCare Services

As your business rapidly evolves, it is critical to advance your security capabilities as well. Often though, you do not have expertise within your organization to deploy, operate, and maintain these new capabilities or are up against tight deadlines to implement change. We understand this challenge and help thousands of organizations every year tackle this problem with FortiCare Services.

Our experts provide accelerated implementation of your technology, reliable assistance through advanced support, and proactive care to ensure your success with Fortinet investment. No matter the size or location of your organization, we are ready to provide you with an elevated experience to help you achieve your business goals with superior security and performance.

FortiCare Support

A FortiCare Support contract entitles you not only to receive updates to the FortiNAC firmware, but also receive two important feeds.

1. Network device database update FortiNAC supports more than 2500 switching, wireless, or firewall devices on the market. As new devices are released, FortiNAC's network device database should be updated to reflect these new models. The weekly update from the FortiNAC team will keep your deployment up to date.
2. FortiGuard IoT Service. One of the means that FortiNAC has to identify devices is to use the cloud-look up service hosted by FortiGuard Labs. A FortiCare Support contract entitles you to use that service at no additional cost, giving you access to a database of millions of devices.

Specifications

	FNC-M-550F	FNC-CA-600F	FNC-CA-500F
System			
CPU	AMD EPYC 7413 24 Core, 2.65GHz Base Freq.		Intel Xeon E-2278GE 8 Core 3.3GHz Base Freq.
Memory	32GB DDR4 memory		16GB DDR4 memory
Hard Disk	2× 960GB SSDs		2× 960GB SSDs
BMC	N/A		N/A
Network Interface	1x GbE RJ45 and 4× 10GbE SFP+		4x GbE RJ45
RAID Card	N/A		N/A
RAID Configuration	Software RAID1		
Console Access	RJ45 type COM port for CLI		
Form Factor	1U Rack Mount		
Dimensions			
Height x Width x Length (inches)	1.73" x 17.20" x 24"		1.73" x 17.32" x 19.69"
Height x Width x Length (mm)	44 × 437 × 610		44 × 440 × 500
Weight	41 lbs (18.6 kg)		32 lbs (14.51 kg)
Environment			
Power Supply	Hot Plug, 1+1 Redundant PSU		Hot Plug, 1+1 Redundant PSU
Input Power	225 watt		174 Watt
Input Current	2.3A@100V, 0.94A@240V		1.5A@100V; 0.625A@240V
Cooling	5x system fans		4x system fans
Panel Display	N/A		N/A
Heat Dissipation	767.731867425 BTU/h		511.82124495 BTU/h
Operation Temperature Range	32°-104°F (0°-40°C)		32°-104°F (0°-40°C)
Storage Temperature Range	-4°-158°F (-20°-70°C)		-4°-158°F (-20°-70°C)
Humidity (Operating) **Humidity (Non-operating)**	5% to 90% non-condensing		5% to 90% non-condensing
Certification			
Safety	Certified as applicable by Product Safety authorities worldwide, including United States (NRTL), Canada (SCC), and European Union (CE).		
Electromagnetic (EMC)	Certified as applicable by EMC authorities worldwide, including United States (FCC), Canada (ICES), and European Union (CE).		
Materials	Certified as applicable by Materials authorities worldwide, including European Union (ROHS) and China (ROHS).		

* The console port can be used for access if the appliance has an issue i.e. you can connect a monitor and a keyboard to it. FortiNAC does not use the console port for access

Specifications

	FNC-CA-700F
System	
CPU	AMD EPYC 7543P 32 Core, 2.8GHz Base Freq.
Memory	96GB DDR4 memory
Hard Disk	2× 960GB SSDs
BMC	N/A
Network Interface	1x GbE RJ45 and 4× 10GbE SFP+
RAID Card	N/A
RAID Configuration	Software RAID1
Console Access	RJ45 type COM port for CLI
Form Factor	1U Rack Mount
Dimensions	
Height x Width x Length (inches)	1.73 × 17.20 × 24
Height x Width x Length (mm)	44 × 437 × 610
Weight	41 lbs (18.6 kg)
Environment	
Power Supply	Hot Plug, 1+1 Redundant PSU
Input Power	375 Watt
Input Current	3.75A@100V, 1.57A@240V
Cooling	5x system fans
Panel Display	N/A
Heat Dissipation	1279.553112375 BTU/h
Operation Temperature Range	32°-104°F (0°-40°C)
Storage Temperature Range	-4°-158°F (-20°-70°C)
Humidity (Operating) **Humidity (Non-operating)**	5% to 90% non-condensing
Certification	
Safety	Certified as applicable by Product Safety authorities worldwide, including United States (NRTL), Canada (SCC), and European Union (CE).
Electromagnetic (EMC)	Certified as applicable by EMC authorities worldwide, including United States (FCC), Canada (ICES), and European Union (CE).
Materials	Certified as applicable by Materials authorities worldwide, including European Union (ROHS) and China (ROHS).

* The console port can be used for access if the appliance has an issue i.e. you can connect a monitor and a keyboard to it. FortiNAC does not use the console port for access.

Hardware Server Sizing

Appliance

HARDWARE			
Hardware Server	**Type**	**Target Environment**	**Capacity[1]**
FortiNAC-CA-500F	Standalone Appliance (Integrated Control Server and Application Server)	Small Environments	Manages up to 5000 ports in the network
FortiNAC-CA-600F	High Performance Control and Application Server	Medium Environments	Manages up to 15 000 ports in the network
FortiNAC-CA-700F	Ultra High Performance Control and Application Server	Large Environments with few Persistent Agents	Manages up to 25 000 ports in the network
FortiNAC-M-550F	Management Appliance (Provides centralized management when multiple appliances are deployed)	Multi-site environments with multiple appliances	Can manage up to 50 CA servers with latencies up to 600ms in lab environment

1 Ports in the network = total number of switch ports + maximum number of concurrent wireless connections. FortiNAC sizes the appliance capacity based on total port counts not total number of devices.

VM Server Resource Sizing

Virtual

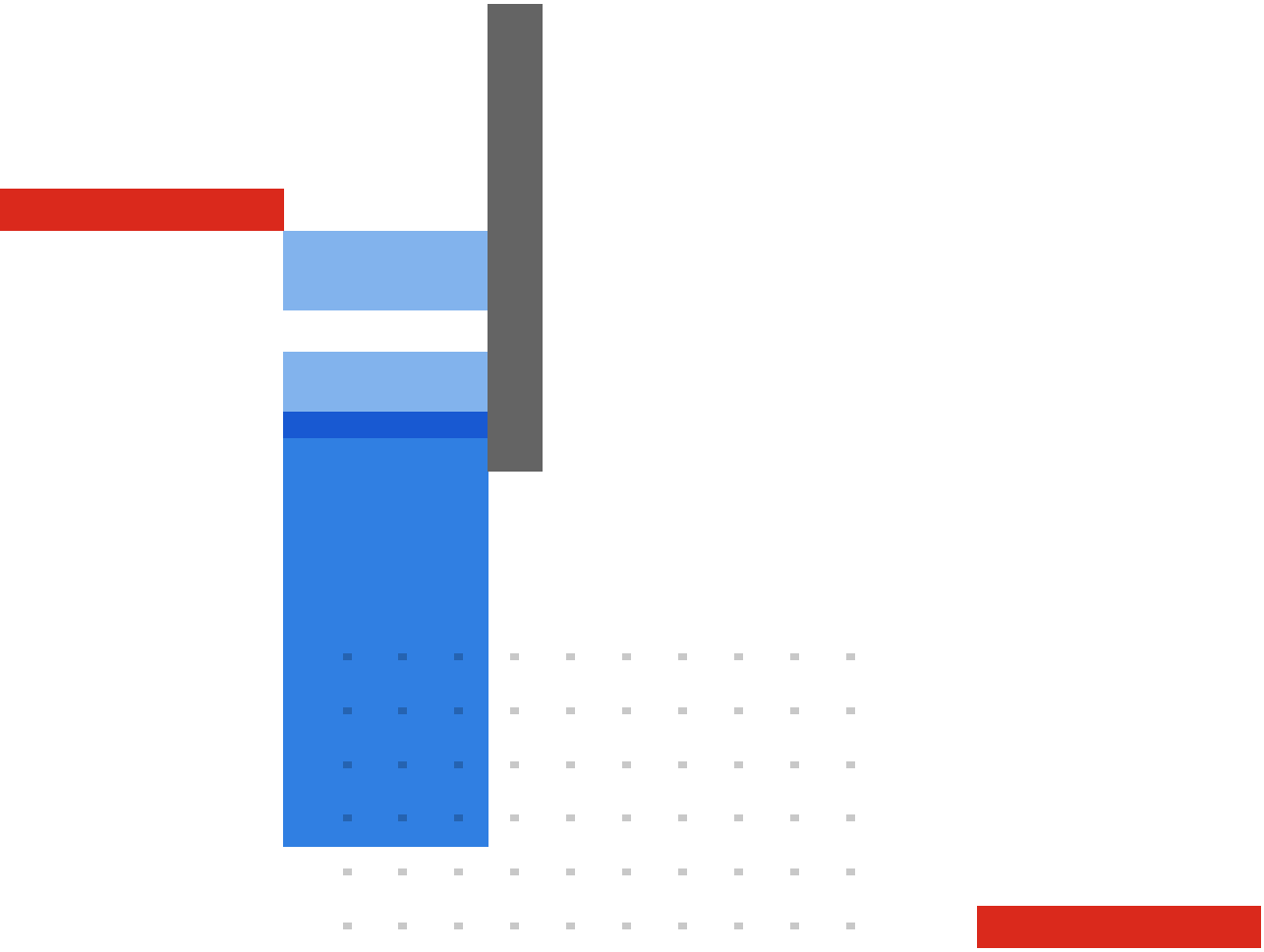
VIRTUAL MACHINE							
VM OS	**SKU**	**Ports in the Network[1]**	**Target Environment**	**CPU Reference**	**vCPU Qty[2]**	**Memory (GB)**	**Disk (GB)**
FortiNAC-OS	**FNC-CAX-VM**	Up to 5 000	Small	Intel Xeon E-2278 GE 3.3 GHz 8C/16T	8	16	100
		Up to 15 000	Medium	AMD Milan EPYC 7413 2.65 GHz 24C/48T	24	32	100
		Up to 25 000	Large	AMD Milan EPYC 7543P 2.8 GHz 32C/64T	32	96	100
	FNC-MX-VM	Up to 50 CA Servers	Large	AMD Milan EPYC 7413 2.65 GHz 24C/48T	24	32	100

[1] Ports in the network = total number of switch ports + maximum number of concurrent wireless connections. FortiNAC sizes the appliance capacity based on total ports count, not total number of devices.

[2] The values in the vCPU column were determined by using the CPUs in the CPU reference column and are guidelines only. VM resources may vary based on individual environments.

Ordering Information

PRODUCT	SKU	DESCRIPTION
Appliances		
FortiNAC-CA-500F	FNC-CA-500F	FortiNAC Network Control and Application Server (F Series)
FortiNAC-CA-600F	FNC-CA-600F	FortiNAC High Performance Network Control and Application Server (F Series)
FortiNAC-CA-700F	FNC-CA-700F	FortiNAC Ultra High Performance Network Control and Application Server (F Series)
FortiNAC-M-550F	FNC-M-550F	FortiNAC Network Manager (F Series)
Virtual Machines		
FortiNAC Control and Application extended VM	FNC-CAX-VM	FortiNAC Control and Application eXtended VM Server (VMWare or Hyper-V or AWS or Azure or KVM) (Running FortiNAC-OS)
FortiNAC Manager extended VM	FNC-MX-VM	FortiNAC Manager eXtended VM Server (VMware or Hyper-V or AWS or Azure or KVM) (Running FortiNAC-OS)
Perpetual Licenses		
FortiNAC BASE License 100	LIC-FNAC-BASE-100	FortiNAC BASE License for 100 concurrent endpoint devices. The BASE license provides Endpoint Visibility and Dynamic VLAN Steering.
FortiNAC BASE License 1K	LIC-FNAC-BASE-1K	FortiNAC BASE License for 1K concurrent endpoint devices. The BASE license provides Endpoint Visibility and Dynamic VLAN Steering.
FortiNAC BASE License 10K	LIC-FNAC-BASE-10K	FortiNAC BASE License for 10K concurrent endpoint devices. The BASE license provides Endpoint Visibility and Dynamic VLAN Steering.
FortiNAC BASE License 50K	LIC-FNAC-BASE-50K	FortiNAC BASE License for 50K concurrent endpoint devices. The BASE license provides Endpoint Visibility and Dynamic VLAN Steering.
FortiNAC PLUS License 100	LIC-FNAC-PLUS-100	FortiNAC PLUS License for 100 concurrent endpoint devices. All the functionality of BASE with more advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PLUS License 1K	LIC-FNAC-PLUS-1K	FortiNAC PLUS License for 1K concurrent endpoint devices. All the functionality of BASE with more advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PLUS License 10K	LIC-FNAC-PLUS-10K	FortiNAC PLUS License for 10K concurrent endpoint devices. All the functionality of BASE with more advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PLUS License 50K	LIC-FNAC-PLUS-50K	FortiNAC PLUS License for 50K concurrent endpoint devices. All the functionality of BASE with more advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PRO License 100	LIC-FNAC-PRO-100	FortiNAC PRO License for 100 concurrent endpoint devices. PRO license level provides the ultimate in visibility, control and response.
FortiNAC PRO License 1K	LIC-FNAC-PRO-1K	FortiNAC PRO License for 1K concurrent endpoint devices. PRO license level provides the ultimate in visibility, control and response.
FortiNAC PRO License 10K	LIC-FNAC-PRO-10K	FortiNAC PRO License for 10K concurrent endpoint devices. PRO license level provides the ultimate in visibility, control and response.
FortiNAC PRO License 50K	LIC-FNAC-PRO-50K	FortiNAC PRO License for 50K concurrent endpoint devices. PRO license level provides the ultimate in visibility, control and response.
Subscription Licenses		
Visibility (BASE)	FC1-10-FNAC1-215-01-DD	License for 25 concurrent endpoints. MOQ 500.
	FC2-10-FNAC1-215-01-DD	License for 500 concurrent endpoints. MOQ 500.
	FC3-10-FNAC1-215-01-DD	License for 10K concurrent endpoints. MOQ 500.
Visibility and Control (PLUS)	FC1-10-FNAC1-213-01-DD	License for 25 concurrent endpoints. MOQ 500.
	FC2-10-FNAC1-213-01-DD	License for 500 concurrent endpoints. MOQ 500.
	FC3-10-FNAC1-213-01-DD	License for 10K concurrent endpoints. MOQ 500.
Visibility, Control, and Response (PRO)	FC2-10-FNAC1-209-01-DD	License for 25 concurrent endpoints. MOQ 500.
	FC3-10-FNAC1-209-01-DD	License for 500 concurrent endpoints. MOQ 500.
	FC4-10-FNAC1-209-01-DD	License for 10K concurrent endpoints. MOQ 500.



FORTINET

www.fortinet.com

October 12, 2023

FNC-DAT-R23-20231012