

Cisco Secure Firewall Feature Comparison Matrix v 7.3

Security Business Group
Network Security Technical Marketing Engineering

06 February 2023

Contents

Introduction	2
Platform Selection:	2
ASA Management Selection:	3
FTD Management Selection:	4
Management Features Matrix – ASA	5
Management Features Matrix – FTD	13
Public Cloud Secure Firewall	29
Azure Native vs. Cisco Secure Firewall	29
Public Cloud Secure Firewall	38
Google Cloud vs. Cisco Secure Firewall	38
Public Cloud Secure Firewall	44
AWS Firewall vs. Cisco Secure Firewall	44

Introduction

The purpose of this document is to inform and accelerate our users decision-making when choosing between Cisco ASA or FTD platforms and available management options. More information ASA to FMT migration is available here: [Cisco ASA to FTD using FMT](#)

Platform Selection:

Choose ASA for	Choose FTD for
<ul style="list-style-type: none">• Traditional/Stateful L3-L4 Firewall• Layer 7 Protocol Inspection• Simple 5 tuple-based Access control• CGNAT, QoS, Advanced Routing• VPN only deployment• Remote Access VPN Headend with the following features:<ul style="list-style-type: none">◦ EzVPN/L2TP/3rd Party Clients◦ TACACS/Kerberos◦ Clientless VPN has been deprecated with 9.17 release• Multi-context firewall <p>Management Features Matrix – ASA</p>	<ul style="list-style-type: none">• Next-Gen Firewall and IPS (NGFW, NGIPS)• Advanced Malware Protection (AMP)• True multi-tenancy with multi-Instance• Advanced network visibility and threat analytics<ul style="list-style-type: none">◦ Correlation Rules◦ Custom IPS Rules◦ Firepower Recommendations• Incident response and threat investigation• TLS decryption, Encrypted traffic visibility• VPN and NGFW/NGIPS functionality on one box• Dynamic Objects/Attribute Based Policy• WAN Connect Use Case (DIA, Auto Tunnel)• Workload Integration <p>Management Features Matrix – FTD</p>

ASA Management Selection:

Features	CSM	ASDM	CDO
Type of manager	On premise and multi-device	On-box local device	Cloud, multi-device, multi-platform
Firewall Deployment Modes	Active/Standby, Active/Active, Cluster, VPN Load Balancing	Active/Standby, Active/Active, Cluster, VPN Load Balancing	Active/Standby
VPN Management	GUI-based configuration for Secure Client (AnyConnect), Hostscan, Policy and Route Based VPNs	GUI-based configuration for Secure Client (AnyConnect), Hostscan, Policy and Route Based VPNs	CLI and GUI based configuration for Secure Client (AnyConnect), (Hostscan or DAP configurable through CLI/ASDM only), Policy and Route Based VPNs
Firewall Management Automation	Rule Optimization, Shared Configuration, Usage reports	Hit counts and Configuration Wizards	Object Conflicts, Rule Optimization, Configuration templates, CLI Macros
Eventing	Event Viewer and Report manager, Syslog, Netflow to external logging servers , SAL cloud integration using SEC	Event Viewer manager, Syslog, Netflow to external logging servers SAL cloud integration using SEC	Event Viewer and Enhanced VPN monitoring and reporting, SAL Cloud integration with Cross Launch

FTD Management Selection:

Features	FMC	FDM	cloud-delivered FMC/CDO
Type of manager	On premise and multi-device	On-box local device	Cloud, multi-device, multi-platform
Type of Device	NGFW, NGIPS	NGFW	NGFW, NGIPS (in cdFMC) ASA, Meraki, AWS VPC (in CDO)
Deployment Mode	High Availability, Clustering, Multi-Instance	High Availability	High Availability, Multi-instance, Cluster
Contextual Visibility	Network Discovery, Application and user visibility, Host profiles, Dynamic Objects	Application and user visibility	Application and user visibility, Host profiles generated by Analytics from SAL
Access Controls	Prefilter Rules, SI, Identity Policy, Granular IPS and Malware Policies, URL and Application Filtering, L2-L7 rules, Dynamic Objects, Encrypted Flow Visibility, QUIC detection, TLS1.3 decryption	TLS1.3 Server Identity Discovery, SI, Identity Policy, Granular IPS and Malware Policies, URL and Application Filtering, L3-L7 rules, TLS1.3 decryption	Prefilter Rules, SI, Identity Policy, Granular IPS and Malware Policies, URL and Application Filtering, L2-L7 rules, Dynamic Objects, Encrypted Flow Visibility, QUIC detection, TLS1.3 decryption
Simplified Branch	Application Aware Routing, Loopback Interface, DVTI, Link Health Monitoring, DIA, ECMP, Dual ISP, Data interface for Management	ECMP, Dual ISP	Application Aware Routing, Loopback Interface, DVTI, Link Health Monitoring, DIA, ECMP, Dual ISP, Data interface for Management
Threat Intelligence	Talos, 3 rd party feeds using CTID, 3 rd party vulnerability databases, MITRE info in Events	Talos	Talos, Additional Threat Intelligence through SAL integration, MITRE focused Analytics alerts
Automation	Firepower recommendations, Correlation Rules, Rapid Threat Containment, CTID, SecureX Orchestration automation workflow	Wizard based configuration, contextual help,	Rapid Threat Containment, SecureX Orchestration automation workflows
Eventing	FMC, Syslog, eStreamer, Cisco Secure Logging and Analytics OnPrem and SaaS	FDM, Syslog, Cisco Secure Logging and Analytics SaaS	Cisco Secure Logging and Analytics SaaS (90-day storage up to 3 years), Syslog, Hybrid Logging with on-prem FMC
Analytics and Threat investigation	FMC for dashboard and analytics, SecureX	SecureX	SecureX, Cisco Secure Logging and Analytics, Summary dashboard in CDO

Management Features Matrix – ASA

LEGEND
Matured, tested, and verified
Deprecated
Not Supported

Features	Cisco Security Manager (4.26)	Adaptive Security Device Manager (7.19)	Cisco Defense Orchestrator (Jan 2023)
Management Features			
Location and type of manager	Off-box Centralized Manager for up to 2500 ASAs (Based on deployment scenario).	Java Based, Integrated on-box manager for single device. Available free with every ASA image	Cloud-Based Manager for ASA, FTD, Meraki, AWS VPC and IOS devices. Subscription based on managed device. ASA can be co-managed with ASDM
Managed Devices	Manages ASAs including ASAs that have a FP module	Available on all form factors running ASA software	FP1000, FP2100, FP4100 and FP9300 hardware running ASA, ASAv, ISA 3000, Cisco Secure Firewall Cloud Native Support
Available Form Factors	Client-server application installed on Windows server.	Java based application	Cloud based web application
Multi Tenancy	X	X	✓ (Also offers a dedicated MSP Portal)
Management Authentication	✓	✓	SAML 2FA -- Cisco provided (Cisco Secure Sign-On) or Roll Your Own
Management RBAC (Authorization)	✓	✓	Super Admin, Admin, Read-Only, Deploy-Only, Edit-Only, VPN Session Manager role
Management Audit (Accounting)	✓	✓	✓
Deployment History	✓	X	✓
Pending Changes	✓	✓	✓
Policy Compare	✓	X	✓
Configuration Archive	✓	X	✓
OOB Change Detection	✓ (Configurable, option to discard)	✓ (Not Configurable)	✓ (Configurable, option to discard)
Integration with AWS Guard Duty	CLI Only	CLI Only	CLI Only
Global Search	X	X	✓

Features	Cisco Security Manager (4.26)	Adaptive Security Device Manager (7.19)	Cisco Defense Orchestrator (Jan 2023)
Firewall Operating Mode Features			
Stateful Transparent Firewall	✓	✓	CLI Only
Stateful Routed Firewall	✓	✓	✓
Scalability and High Availability Features			
Active/Active Failover	✓	✓	✓
Active/Standby Failover	✓	✓	✓
Clustering on Virtual form factor (VMWare and KVM)	✓	✓	X (Only CLI)
Clustering on 5500-X	✓	✓	X (Only CLI)
Inter-Chassis and Intra-Chassis Clustering on 4100/9300 Appliance	✓	✓	X (Only CLI)
Integrate with AWS Gateway LB	✓	X	X (Only CLI)
Clustering on AWS	✓	X	X (Only CLI)
Hardware Specific Features			
Fail to wire interfaces	✓	✓	✓
ASA & FTD in 9300 (different SMs)	(Only ASA)	(Only ASA)	✓
Stateful Firewall Features			
Initial Setup Wizard	Has a Jumpstart Wizard to help with initial configuration	12 step Startup Wizard for Interfaces/NAT/DHCP/etc connectivity for the ASA	Cloud-native onboarding for FTD - no need for on-prem SDC. Useful when mgmt IP is DHCP assigned and for branches. Simple Secure Device Connector (SDC) Setup (vAPP if using the VMWare image), and then easy onboarding of devices
Interfaces	✓	✓	✓

Features	Cisco Security Manager (4.26)	Adaptive Security Device Manager (7.19)	Cisco Defense Orchestrator (Jan 2023)
Stateful Firewall Object Features			
Object based ACL	✓	✓	✓
IP address objects (v4 & v6)	✓	✓	✓
Object groups	✓	✓	✓
Groups of groups	✓	✓	✓
UDP and TCP ports in one object	✓	✓	✓
Address ranges	✓	✓	✓
Port ranges	X	X	X
Object change history	✓	X	✓
Find unused objects	✓	X	✓
IP object based on a host/domain name (FQDN object)	✓	✓	✓
Classic Firewall Features			
Access Ctrl rules (IP, port)	✓	✓	✓
Integrated routing and Bridging in the same context	✓	✓	✓
TCP State bypass	✓	✓	✓
Only packets that belong to established sessions can be allowed through the firewall	✓	✓	✓
TCP Sequence random.	✓	✓	✓
Connection limits and TCP Intercept	✓	✓	✓
Dead Connection Detection	✓	✓	✓

Features	Cisco Security Manager (4.26)	Adaptive Security Device Manager (7.19)	Cisco Defense Orchestrator (Jan 2023)
Advanced Protocol Inspection Features			
SIP	✓	✓	✓
FTP	✓	✓	✓
DNS	✓	✓	✓
DCE-RPC	✓	✓	✓
GTP	✓	✓	✓
H323 (H225, RAS)	✓	✓	✓
ICMP	✓	✓	✓
NetBIOS	✓	✓	✓
RTSP	✓	✓	✓
SCCP	✓	✓	✓
RSH	✓	✓	✓
ESMTP	✓	✓	✓
SQLNET	✓	✓	✓
SUNRPC	✓	✓	✓
XDMCP	✓	✓	✓
TFTP	✓	✓	✓
Stateful Firewall Other Features			
NAT	✓	✓	✓
FQDN based NAT	✓	✓	X
Routing	✓	✓	✓
Path Monitoring Metrics for PBR egress interface selection	✓	✓	X

Features	Cisco Security Manager (4.26)	Adaptive Security Device Manager (7.19)	Cisco Defense Orchestrator (Jan 2023)
VPN -> Site-to-Site Features			
IKEv1, IKEv2	✓	✓	Allows onboarding of ASAs with S2S VPN configured. Can be used to monitor tunnel status. Configuration allowed only for SASE tunnel to Umbrella.
Static, Dynamic Peering	✓	✓	✓
IPv4, IPv6 Addressing	✓	✓	✓
PSK Authentication	✓	✓	✓
Certificate Authentication	✓	✓	X (CLI/ASDM only)
Policy Based VPN	✓	✓	✓
Route Based VPN	✓	✓	✓
Static and Dynamic VTI	✓	✓	X (CLI/ASDM only)
Loopback Support	✓	✓	X (CLI/ASDM only)
Monitoring	✓	✓	✓
VPN -> Remote Features			
Connection Protocol	✓	✓	✓
AnyConnect Client	✓	✓	✓
3rd Party Client	✓	✓	X (CLI/ASDM only)
Dual Stack IPv4/v6 (3 rd party and AnyConnect)	✓	✓	X (CLI/ASDM only)
Authentication Protocol	✓	✓	✓
Passwordless Authentication (WebAuthN)	X	✓	X (CLI/ASDM only)
Certificate Authentication	✓	✓	✓
TLS 1.3	✓	✓	X (CLI/ASDM only)
2FA/MFA	✓	✓	✓
Authorization Protocol	✓	✓	✓
Accounting Protocol	✓	✓	✓
DAP/HostScan	✓	✓	X (CLI/ASDM only)
ISE Posture & CoA	✓	✓	X (CLI/ASDM only)

Features	Cisco Security Manager (4.26)	Adaptive Security Device Manager (7.19)	Cisco Defense Orchestrator (Jan 2023)
AnyConnect Profile Attributes	✓	✓	✓
Monitoring	✓	✓	✓ (Client Geolocation info and ability to terminate VPN sessions with VPN Session Manager)
VPN Load Balancing	✓	✓	X
IPSEC Offload (3100 series)	✓	✓	X
SAML with cert auth	✓	✓	X
Layer 2 - 7 Access Control Filter Features			
IP address	✓	✓	✓
VLAN	✓	✓	✓
User ID / User Group	✓	✓	✓
Ports	✓	✓	✓
Protocol	✓	✓	✓
Objects	✓	✓	✓
SGT	✓	✓	✓
Trusting Traffic / No inspection	✓	✓	✓
Tunnel Policies	✓	✓	✓
NGFW Identity Awareness & Control Features			
Passive authentication	✓	✓	✓
Active Authentication/Captive Portal/Cut Through Proxy and Direct Authentication	✓	✓	✓
Enforce traffic policy by SGT	✓	✓	✓
Read SGT from packets	✓	✓	✓
Rapid Threat Containment using ISE	X	X	X

Features	Cisco Security Manager (4.26)	Adaptive Security Device Manager (7.19)	Cisco Defense Orchestrator (Jan 2023)
NGFW Layer 4 - 7 Firewall Functionality Features			
Application Control	X	X	X
Limit bandwidth by user/application (Rate Limiting)	X	X	X
URL Filtering	X	X	X
SSL Decryption in software	X	X	X
SSL Decryption in hardware	X	X	X
OpenAppID	X	X	X
AMP For networks	X	X	X
ThreatGRID Dynamic Analysis	X	X	X
Threat/Risk Reports	X	X	X
Web SafeSearch and YouTube Edu	X	X	X
TLS Proxy for Encrypted Voice Inspection	X	X	X
Web Cache Services Using WCCP	✓	✓	✓
Pre-filter Policy (Tunneled & Fastpath)	✓	✓	✓
Firewall Management Automation			
Hit Counts	✓	✓	✓
Rule Conflict Detection (Redundant & Shadowed)	✓	X	✓
Object Conflict detection	X	X	✓

Features	Cisco Security Manager (4.26)	Adaptive Security Device Manager (7.19)	Cisco Defense Orchestrator (Jan 2023)
Logging & Analytic Features			
Log connections to management console	✓	✓	✓
Send syslogs- from the management console	✓	✓	✓
Send syslogs - directly from the device	✓	✓	✓
Security Analytics and Logging	✓ (Event viewer is in CDO with Analytics in SWC)	✓ (Event Viewer is in CDO with Analytics in SWC)	✓
Dashboards	✓	✓	X
Reporting	✓	X	✓
eStreamer	X	X	X
CEF	X	X	X
NetFlow	✓	✓	✓
SecureX Integration	X	X	✓
Risk Reports/SRA	X	X	X
Notification Service	X (Only UI)	X (Only UI)	✓ (Email alerts and UI notifications)
Device Health Report	✓	✓	X

Features	Cisco Security Manager (4.26)	Adaptive Security Device Manager (7.19)	Cisco Defense Orchestrator (Jan 2023)
APIs			
REST API	✓	✓	✓
Workflows (Submitter, Approver, Deployer)	✓	X	✓
Ticket Management System Integration	✓	X	✓
ASA to FTD Migration	✓	X	✓

Management Features Matrix – FTD

LEGEND
Matured, tested, and verified
Deprecated
Not Supported

Features	Firepower Management Center (7.3)	Firepower Device Manager (7.3)	Cloud-delivered FMC in CDO (January 2023)
Management Features			
Location and type of manager	Web-based, Off-box Centralized Manager for up to 750 Sensors (Based on FMC Appliance model). Use in conjunction with CSM to manage ASAs in the case of ASA w/ FP services	Simple, Web-based, Intuitive, Integrated on-box manager for single device. Available free with every FTD image Co-management with CDO-FDM management, no co-management with FMC	SaaS based Centralized Manager for up to 1000 Sensors – service upkeep managed and maintained by Cisco
Managed Devices	5508-X,5516-X, FP1000, FP2100, FP3100, FP4100 and FP9300 hardware running FTD , ISA 3000, FTDv in VMWare, KVM, Azure, AWS, GCP, OCI (Autoscale supported for GCP,OCI, AWS and Azure along with Accelerated Networking in Azure), Nutanix, OpenStack, HyperFlex ASA with FP Services FP 7000 and 8000 appliances	Any ASA, FP1000, FP2100, FP4100 and FP9300 hardware running FTD VMWare, KVM, ISA 3000, FTDv in GCP, Azure and AWS	5508-X,5516-X, FP1000, FP2100, Secure Firewall 3100, FP4100 and FP9300 hardware running FTD , ISA 3000, FTDv in VMWare, KVM, Azure, AWS, GCP, OCI, Nutanix, OpenStack, HyperFlex Running version 7.2 and above (Supported for devices running 7.0 with patch)
Available Form Factors	FMC1600, FMC 2600, FMC4600 FMCv2/10/25 (VMware, KVM, AWS, Azure, GCP, OCI, Nutanix, Hyperflex, OpenStack) FMCv300 (VMware, AWS , Azure, KVM and OCI)	On box on Physical FTDs, FTDv running on VMWare, KVM, AWS, Azure, GCP, OCI, Nutanix, OpenStack, HyperFlex	Cloud based web application
High Availability	FMC HA in all hardware models, VMWare, AWS, Azure, KVM and OCI	X	✓ (cloud based redundancy) DR across Availability zones, within the same availability zone, daily snapshot
Multi Tenancy	✓ FMC Domains	X	✓ (true separate cloud tenants) with a unified multi-tenant management portal – no FMC domains
Management Authentication	Local, AD, Radius, also allows to specify a real name for a user account, SAML SSO	Local Admin and RADIUS	SAML 2FA -- Cisco provided (Cisco Secure Sign-On) or Roll Your Own

Features	Firepower Management Center (7.3)	Firepower Device Manager (7.3)	Cloud-delivered FMC in CDO (January 2023)
Management RBAC (Authorization)	Granular RBAC provided locally, SAML SSO	Available w/ RADIUS authentication Roles: RO, RW and Admin	Super Admin, Admin, Read-Only, Edit-Only, Deploy-Only
Management Audit (Accounting)	Audit Logs. report can be generated from these logs in HTML, PDF and CSV formats	✓	Audit Logs. report can be generated from these logs in HTML, PDF and CSV formats (Changelog for configuration changes in CDO on roadmap)
Deployment History	✓ Audit Log support Routing Policies, FTD Platform Settings, VPN, DHCP, DDNS, Pre-Filter Policies, QoS Policies, Objects (Network, Port, URL, VLAN Tag)	✓	✓ Audit Log support Routing Policies, FTD Platform Settings, VPN, DHCP, DDNS, Pre-Filter Policies, QoS Policies, Objects (Network, Port, URL, VLAN Tag)
Pending Changes	- High level indication in Deploy Policies window - Audit Log support Routing Policies, FTD Platform Settings, VPN, DHCP, DDNS, Pre-Filter Policies, QoS Policies, Objects (Network, Port, URL, VLAN Tag)	✓	- High level indication in Deploy Policies window - Audit Log support Routing Policies, FTD Platform Settings, VPN, DHCP, DDNS, Pre-Filter Policies, QoS Policies, Objects (Network, Port, URL, VLAN Tag)
Policy Compare	- Available for DNS, File, Health, Identity, Intrusion, Network Analysis, SSL policies - Audit Log support Routing Policies, FTD Platform Settings, VPN, DHCP, DDNS, Pre-Filter Policies, QoS Policies, Objects (Network, Port, URL, VLAN Tag)	✓	- Available for DNS, File, Health, Identity, Intrusion, Network Analysis, SSL policies - Audit Log support Routing Policies, FTD Platform Settings, VPN, DHCP, DDNS, Pre-Filter Policies, QoS Policies, Objects (Network, Port, URL, VLAN Tag)
Configuration Archive	✓	✓	✓
Bulk Edit	✓	X	✓
Advanced Search	✓	X	✓
Object-group rule optimization	✓	✓	✓
Interface Object Optimization	✓ (Native and MI)	X	✓ (Native and MI)
Time Based Rules	✓	✓ (API)	✓
Selective Deployment	✓	X	✓
Config Rollback	✓	X (You can discard undeployed changes)	✓
Move Rules within Policy	✓	✓	✓

Features	Firepower Management Center (7.3)	Firepower Device Manager (7.3)	Cloud-delivered FMC in CDO (January 2023)
Move Rules across Policies	✓	X	✓
Rule Sets (set of rules shared by multiple FTDs)	✓ (You can create category and club rules under them but they can't be shared across policies)	X	✓ (You can create category and club rules under them but they can't be shared across policies)
Remote Branch Deployment (Using Data interface for Management)	✓ (Standalone and HA)	✓	✓ (Standalone and HA)
Bulk Upgrade	✓	X (On box single device manager)	✓
Revert Upgrade	✓ (Major and Maintenance upgrades)		✓ (Major and Maintenance upgrades)
Notification Service	✓ (Only UI)	✓ (only UI)	UI and Email Alerts
Firewall Operating Mode Features			
Stateful Transparent firewall	✓	X	✓
Stateful Routed firewall	✓	✓	✓
Multi-Instance	✓	X	✓
Scalability and High Availability Features			
Active/Standby Failover	✓	✓	✓
Clustering on Virtual form factor (Azure, GCP, AWS, VMWare and KVM)	✓	X	✓
Intra-Chassis Clustering on Firepower Appliance (9300)	✓	X	✓
Inter-Chassis Clustering on Firepower Appliance (4100/9300)	✓	X	✓
Multi-Instance Clustering (4100/9300)	✓	X	✓
Integrate with AWS Gateway LB	✓	X	✓
Integrate with Azure Gateway Load Balancers	✓		✓

Features	Firepower Management Center (7.3)	Firepower Device Manager (7.3)	Cloud-delivered FMC in (January 2023)
Hardware Specific Features			
Flow Offload on 9300 and 4100	✓	✓	✓
Fail to wire interfaces	✓	✓ (Inline sets not supported)	✓
ASA & FTD in 9300 (different SMs)	(Only FTD)	(Only FTD)	(Only FTD)
L2 switchports and PoE in 1010	✓	✓	✓
Stateful Firewall Features			
Initial Setup Wizard	Improved initial setup experience: <ul style="list-style-type: none"> - Default boot protocol set to DHCP (Support for Non-DHCP environments) - UI or CLI based configuration (3 steps) - Change password - Accept EULA - Configure Network Bootstrap CLI for remote management on data interface 	3 step Easy Setup Wizard: <ul style="list-style-type: none"> - Outside/DHCP/NTP connectivity for the FTD - Create default for NAT and Routing in the background. - Creates default deny ACL Rule - Has a Live topology display that changes color as it progresses 	Cloud-native onboarding for FTD using registration key. Low touch Provisioning upon device bootup using device S/N
Interfaces	✓	Except Redundant, Inline interfaces	✓

Features	Firepower Management Center (7.3)	Firepower Device Manager (7.3)	Cloud-delivered FMC in (January 2023)
Stateful Firewall Object Features			
Object based access control policy	✓	✓	✓
IP address objects (v4 & V6)	✓	✓	✓
Object groups	✓	✓	✓
Groups of groups	✓	✓	✓
UDP and TCP ports in one object	✓	✓	✓
Address ranges	✓	✓	✓
Port ranges	✓	✓	✓
Object change history	✓	✓	✓
Find unused objects	✓	X	✓
IP object based on a host/domain name (FQDN object)	✓	✓	✓

Features	Firepower Management Center (7.3)	Firepower Device Manager (7.3)	Cloud-delivered FMC in (January 2023)
Object Support			
IPv4 Private-Use - All RFC1918	✓	✓	✓
IPv4 Private-Use - 10/8	✓	✓	✓
IPv4 Private-Use - 172.16/12	✓	✓	✓
IPv4 Private-Use - 192.168/16	✓	✓	✓
IPv6 Private-Use - Unique Local Addresses	✓	✓	✓
IPv4 Link-Local	✓	✓	✓
IPv6 Link-Local	✓	✓	✓
IPv4 Multicast	✓	✓	✓
IPv6 to IPv4 Relay Anycast	✓	✓	✓
IPv4 Benchmark Tests	✓	✓	✓
IPv6 - IPv4 Mapped	✓	✓	✓
any ipv4	✓	✓	✓
any ipv6	✓	✓	✓
any both (our keyword any)	✓	✓	✓

Features	Firepower Management Center (7.3)	Firepower Device Manager (7.3)	Cloud-delivered FMC in (January 2023)
Classic Firewall Features			
Acc. ctrl rules (IP, port)	✓	✓	✓
Integrated routing and Bridging in the same context	✓	✓	✓
TCP State bypass	✓	Flexconfig	✓
Only packets belonging to established sessions allowed	✓	Flexconfig	✓
TCP Sequence randomization	✓	Flexconfig	✓
Connection limits and TCP Intercept	✓	Flexconfig	✓
Dead Connection Detection	Flexconfig	Flexconfig	Flexconfig

Features	Firepower Management Center (7.3)	Firepower Device Manager (7.3)	Cloud-delivered FMC in (January 2023)
Advanced Protocol Inspection Features			
SIP	✓	Flexconfig	✓
FTP	✓	Flexconfig	✓
DNS	✓	Flexconfig	✓
DCE-RPC	✓	Flexconfig	✓
5G (GTP,M3UA,Diameter, SCTP)	✓ (requires Carrier License)	X	✓ (requires Carrier License)
H323 (H225, RAS)	✓	Flexconfig	✓
ICMP	✓	Flexconfig	✓
NetBIOS	✓	Flexconfig	✓
RTSP	✓	Flexconfig	✓
SCCP	✓	Flexconfig	✓
RSH	✓	Flexconfig	✓
ESMTP	✓	Flexconfig	✓
SQLNET	✓	Flexconfig	✓
SUNRPC	✓	Flexconfig	✓
XDMCP	✓	Flexconfig	✓
TFTP	✓	Flexconfig	✓
Stateful Firewall Other Features			
NAT	Firepower NAT also included	✓	Firepower NAT also included
FQDN based NAT	✓	✓	✓
Routing	OSPF, EIGRP, BGP, RIP, Multicast, Static, Route Tracking(SLA) – Supported on UI PBR, ISIS, BFD, ECMP Only API for static route, VRF, Application based Routing (DIA)	Static and Route Tracking(SLA) on UI OSPF, BGP and respective route object – SmartCLI Global EIGRP – FDM UI Multicast, Interface EIGRP , PBR – FlexConfig APIs available for Static Route, OSPF, BGP and generic Flexconfig, VRF, ECMP	OSPF, EIGRP, BGP, RIP, Multicast, Static, Route Tracking(SLA) – Supported on UI PBR, ISIS, BFD, ECMP Only API for static route, VRF, Application based Routing (DIA)

Features	Firepower Management Center (7.3)	Firepower Device Manager (7.3)	Cloud-delivered FMC in (January 2023)
VPN -> Site-to-Site Features			
IKEv1, IKEv2	✓	✓	✓
Static, Dynamic Peering	✓	✓	✓
IPv4, IPv6 Addressing	✓	✓	✓
PSK Authentication	✓	✓	✓
Certificate Authentication	✓	✓	✓
Policy Based VPN (Crypto Map)	✓	✓	✓
Route Based VPN (VTI)	✓	✓	✓
Static, Dynamic and Backup VTI	✓		✓
Loopback Interface	✓	X	✓
Monitoring	✓	X	✓
Dynamic RRI	✓	X (Only FTD API)	✓
Umbrella SIG Auto-Tunnel	✓	X	✓

Features	Firepower Management Center (7.3)	Firepower Device Manager (7.3)	Cloud-delivered FMC in (January 2023)
VPN -> Remote Features			
Connection Protocol	TLSv1.2, TLSv1.3, IKEv2, DTLS	TLSv1.2, IKEv2, DTLS	TLSv1.2, TLSv1.3, IKEv2, DTLS
AnyConnect Client	✓	✓	✓
Clientless VPN	X	X	X
3rd Party Client	X	X	X
Authentication Protocol	RADIUS, LDAP, Local, SAML	RADIUS, LDAP, Local, SAML	RADIUS, LDAP, Local, SAML
Passwordless Authentication (WebAuthN)	✓	✓	✓
Certificate Authentication	✓ (Multi Cert too)	✓	✓ (Multi Cert too)
2FA/MFA	✓	✓	✓
Authorization Protocol	RADIUS, LDAP, SAML, SAML & Certificate	RADIUS, LDAP	RADIUS, LDAP, SAML, SAML & Certificate
Accounting Protocol	RADIUS	RADIUS	RADIUS
DAP/HostScan	✓	X (FTD API)	✓
ISE Posture & CoA	✓	✓	✓
AnyConnect Profile Attributes	Flexconfig	Flexconfig	Flexconfig
AnyConnect Management Tunnel	✓	X	✓
AnyConnect Modules	✓	X (FTD API)	✓
AnyConnect Custom Attributes	✓	X	✓
Monitoring	✓ (Additional Client Geolocation info and ability to terminate VPN sessions with VPN Session Manager)	✓	✓ (Additional Client Geolocation info and ability to terminate VPN sessions with VPN Session Manager)
VPN Load Balancing	✓	X	✓
IPSEC Offload (3100 series)	✓	✓ (FlexConfig CLI)	✓
SAML with cert auth	✓	✓	✓

Features	Firepower Management Center (7.3)	Firepower Device Manager (7.3)	Cloud-delivered FMC in (January 2023)
Layer 2 - 7 Access Control Filter Features			
Zone (a logical group of physical or virtual interfaces)	✓	✓	✓
IP address	✓	✓	✓
Geolocation	✓	✓	✓
VLAN	✓	✓	✓
User ID / User Group	✓	✓	✓
VDI user identity	✓	X	✓
ApplD	✓	✓	✓
Ports	✓	✓	✓
Protocol	✓	✓	✓
URL	✓	✓	✓
Objects	✓	✓	✓
SGT	✓	✓	✓
Device type (ISE)	✓	✓	✓
Location IP (ISE)	✓	✓	✓
Trusting Traffic / No inspection	✓	✓	✓
Tunnel Policies	X	X	X
X-Forwarded-For policy	✓	X	✓
Advanced Access Control Features			
Network Discovery	✓	X	X
Application Discovery	✓	X	X
User Discovery	✓	X	X
Indicators Of Compromise, Impact Analysis, Firepower recommendation, etc.	✓	X	X

Features	Firepower Management Center (7.3)	Firepower Device Manager (7.3)	Cloud-delivered FMC in (January 2023)
NGFW Identity Awareness & Control Features			
Passive authentication	✓	✓	✓
Active Authentication/Captive Portal/Cut Through Proxy and Direct Authentication	✓	✓	✓
Enforce traffic policy by SGT	✓	✓	✓
Read SGT from packets	✓	✓	✓
Rapid Threat Containment using ISE	✓	X	✓
Device Level Subnet Filtering	✓ (CLI command)	X	✓ (CLI command)
AD Realm Sequence	✓	✓	✓
PxGrid 2.0 support	✓	✓	✓
Dynamic Object and CSDAC (VMWare, AWS, Azure, O365 and Azure Tags)	✓	X	✓ (CSDAC option within CDO)
Workload Policy Integration	✓	X	✓
Cross Domain for AD domains	✓	X	✓
Source Fire User Agent	Deprecated starting 6.7	Deprecated starting 6.7	Deprecated starting 6.7

Features	Firepower Management Center (7.3)	Firepower Device Manager (7.3)	Cloud-delivered FMC in (January 2023)
NGFW Advanced Inspection Features			
Snort - best in class IPS	✓	✓	✓
Snort3	✓	✓	✓
Normalization and inspection of traffic up to application layer for anti-evasion	✓	✓	✓
Custom IPS Rules	✓	✓	✓
Elephant Flow Visibility	✓	✓	✓
FQDN based Security intelligence feeds	✓	✓	✓
DNS Inspection and sink holing	✓	X	✓
DNS reputation based filtering	✓	✓	✓
File Archive support (zip, rar..)	✓	✓	✓
File pre-classification and local malware inspection	✓	✓	✓
IoC Update Feed	✓	X	✓
Trusted DNS Servers	✓	X	✓
Wildcard Masks	✓	X	✓
Detect HTTP/3 and SMB over QUIC	✓		✓

Features	Firepower Management Center (7.3)	Firepower Device Manager (7.3)	Cloud-delivered FMC in CDO (January 2023)
NGFW Layer 4 - 7 Firewall Functionality Features			
Application Control	✓	✓	✓
Limit bandwidth by user/application (Rate Limiting)	✓	Flexconfig	✓
URL Filtering	✓	✓	✓
SSL Decryption in software	✓ (TLS 1.3 Server Identity Discovery and Encrypted Traffic Visibility well)	✓ (TLS 1.3 Server Identity Discovery as well)	✓
SSL Decryption in hardware	✓	✓	✓
TLS 1.3 Decryption	✓	✓	✓
OpenAppID	✓	✓	✓
AMP For networks	✓	✓	✓
ThreatGRID Dynamic Analysis	✓	X	✓
Threat/Risk Reports	✓	X	X
Web SafeSearch and YouTube Edu	✓	✓	✓
TLS Proxy for Encrypted Voice Inspection	X	X	X
Web Cache Services Using WCCP	Flexconfig	Flexconfig	Flexconfig
Pre-filter Policy (Tunneled & Fastpath)	✓	X	✓
Firewall management automation			
Hit Counts	✓	✓	✓
Rule Conflict Detection (Redundant & Shadowed)	✓	X	✓
Object Conflict detection	X	✓	X
Access control rule conflict analysis	✓	X	✓

Features	Firepower Management Center (7.3)	Firepower Device Manager (7.3)	Cloud-delivered FMC in CDO (January 2023)
Logging and Analytics features			
Log connections to management console	✓	✓	✓
Unified Event Viewer	✓	X	✓
Send syslogs- from the management console	✓	✓	X
Send syslogs - directly from the device	✓	✓	✓
Security Analytics and Logging	✓ (On Prem and Cloud)	✓ (Cloud)	✓ (Cloud)
Dashboards	✓ - Predefined and Customizable dashboard and widgets for network and threat - Limited Device health	✓ - Multiple predefined dashboards for health, network and threat	Dashboards available for: Top Applications Top Attackers Top Destinations Top Targets Top Threats
Reporting	✓ including - Provides templates for reports. - Reports can be exported etc. - Report Designer can convert Dashboard to Reports	X	✓ (High Level Security Report available)
eStreamer	✓	X	X
IBM with QRadar	✓	X	X
CEF	X	X	X
NetFlow	Flexconfig	Flexconfig	Flexconfig
SecureX Integration	✓	✓ (Ribbon not available and no cross launch)	✓
Risk Reports/SRA	✓	X	X
Health Monitoring Functionality	✓	✓	✓ (For FTDs)

Features	Firepower Management Center (7.3)	Firepower Device Manager (7.3)	Cloud-delivered FMC in CDO (January 2023)
APIs			
REST API	✓	FTD APIs available for all FDM	✓ (Uses CDO API Token)
Host Input API	✓	X	✓
Remediation API	✓	X	✓
Database Access API	✓	X	✓
Estreamer API	✓	X	X
Workflows (Submitter, Approver, Deployer)	X	X	X
Ticket Management System Integration	X	X	X
ASA to FTD Migration	✓	Use CDO Tool	✓

Public Cloud Secure Firewall

Azure Native vs. Cisco Secure Firewall

LEGEND
Supported (Yes)
Partial
Not supported (No)

Security Features	FTD 7.3 in Azure	FTD 7.2 in Azure	ASA 9.19 in Azure	ASA 9.18 in Azure	Azure Firewall	Azure Firewall Premium
Site to Site VPN						
IPSec / Site to Site VPN - Hub & Spoke	Yes	Yes	Yes	Yes	Using Azure VPN and Virtual Network Gateway (VNG)	Using Azure VPN and Virtual Network Gateway (VNG)
IPSec / Site to Site VPN - 3rd party / Extranet	Yes	Yes	Yes	Yes	Using Azure VPN and Virtual Network Gateway (VNG)	Using Azure VPN and Virtual Network Gateway (VNG)
PKI support	Yes	Yes	Yes	Yes	Using Azure VPN and Virtual Network Gateway (VNG)	Using Azure VPN and Virtual Network Gateway (VNG)
VTI support	Yes	Yes	Yes	Yes	Using Azure VPN and Virtual Network Gateway (VNG)	Using Azure VPN and Virtual Network Gateway (VNG)
IKEv2 support	Yes	Yes	Yes	Yes	Using Azure VPN and Virtual Network Gateway (VNG)	Using Azure VPN and Virtual Network Gateway (VNG)

Security Features	FTD 7.3 in Azure	FTD 7.2 in Azure	ASA 9.19 in Azure	ASA 9.18 in Azure	Azure Firewall	Azure Firewall Premium
RA VPN						
Clientless-SSL VPN	No	No	Yes	Yes	No	
Anyconnect or Client VPN	Yes	Yes	Yes	Yes	No	
SAML	Yes	Yes	Yes	Yes	No	
MFA-RSA SDI	Yes	Yes	Yes	Yes	No	
MFA-Duo	Yes	Yes	Yes	Yes	No	
Local Auth	Yes	Yes	Yes	Yes	Yes	
RADIUS	Yes	Yes	Yes	Yes	No	
TACACS	No	No	Yes	Yes	No	
Dynamic Access Policy	Yes	Yes	Yes	Yes	No	

Security Features	FTD 7.3 in Azure	FTD 7.2 in Azure	ASA 9.19 in Azure	ASA 9.18 in Azure	Azure Firewall	Azure Firewall Premium
General						
Enterprise FW	Yes	Yes	Yes	Yes	Yes	
App Visibility & Control	Yes	Yes	Cisco ASA can use FQDN (all traffic), ports and protocols.	Cisco ASA can use FQDN (all traffic), ports and protocols.	Azure Firewall only uses FQDN filtering rules (outbound HTTP only), ports and protocols for filtering	Azure Firewall only uses FQDN filtering rules (outbound HTTP only), ports and protocols for filtering
Geolocation	Yes	Yes	No	No	No	
SSL Decryption			No	No	No	TLS configuration is primitive in the Azure Premium Firewall. One CA, and no rules to determine which traffic to decrypt, pass-through or drop. Also, it only supports East-West and Outbound. North-South is supported by the Azure Application Gateway, but this is only HTTPS.
Known key	Yes	Yes	No	No	No	No
Resign	Yes	Yes	No	No	No	Yes
NGIPS / NGIDS	Yes	Yes	No	No	Yes	
Snort 3	Yes	Yes	No	No	No	No
DDoS	No	No	No	No	Azure offers Azure DDoS.	Azure offers Azure DDoS.
URL/Web Filtering	Yes	Yes	No	No	No	Yes
Web Proxy Integration	No	No	No	No	No	No
Advance Malware Protection and Breach Detection	Yes	Yes	No	No	No	No

Security Features	FTD 7.3 in Azure	FTD 7.2 in Azure	ASA 9.19 in Azure	ASA 9.18 in Azure	Azure Firewall	Azure Firewall Premium
Continuous Analysis & Retrospective Detection	Yes	Yes	No	No	No	No
Malware Remediation	Yes	Yes	No	No	No	No
Integrated Sandboxing	Yes	Yes	No	No	No	No
Contextual Awareness (who, what, when, where, why, How)	Yes	Yes	No	No	No	No
User Awareness	Yes	Yes	Yes	Yes	No	
Security Automation & Adaptive Threat Management	Yes	Yes	No	No	Yes	Yes
IoCs	Yes	Yes	No	No	No	No
Network Awareness	Yes	Yes	No	No	No	No
Endpoint Awareness	Yes	Yes	No	No	No	No
Network File Trajectory	Yes	Yes	No	No	No	No
Impact Assessment	Yes	Yes	No	No	No	No
DNS Based Policy & Sinkholing	Yes	Yes	No	No	No	No
Encrypted Traffic Analytics	Yes	Yes	Yes	Yes	No	No
Dynamic Objects	Yes	Yes	No	No	FQDNs and Service Tags only	FQDNs and Service Tags only

Security Features	FTD 7.3 in Azure	FTD 7.2 in Azure	ASA 9.19 in Azure	ASA 9.18 in Azure	Azure Firewall	Azure Firewall Premium
Threat Intelligence						
System Feed (Talos or eq)	Yes	Yes	No	No	Yes	Yes
3rd party - system feed	Yes	Yes	No	No	No	No
3rd party feeds /Threat Intelligence Director / Integrations	Yes	Yes	No	No	Azure Sentinel is a Taxii client	Azure Sentinel is a Taxii client
Automated Intelligence feeds	Yes	Yes	No	No	Yes	Yes
Operational Capabilities						
Software Defined Segmentation	Yes	Yes	Yes	Yes	Yes	
Automatic Threat Containment	Yes	Yes	No	No	Azure triggers can take automated action	Azure triggers can take automated action
Syslog & Event Data Export						
Local / Built into management	Yes	Yes	Yes	Yes	Yes	Yes
Syslog	Yes	Yes	Yes	Yes	Yes	Yes
Reporting Dashboards	Yes	Yes	Yes	Yes	Yes	Yes
SIEM	Yes	Yes	Yes	Yes	Yes	
SOAR	Yes	Yes	Yes	Yes	Yes	
Cisco Threat Response	Yes	Yes	No	No	No	No
SecureX	Yes	Yes	No	No	No	No
Remediation API	Yes	Yes	No	No	No	No
Host API	Yes	Yes	No	No	No	No

Security Features	FTD 7.3 in Azure	FTD 7.2 in Azure	ASA 9.19 in Azure	ASA 9.18 in Azure	Azure Firewall	Azure Firewall Premium
NetOps Features						
High Availability					Yes	Yes
Clustering	Yes	No	No	No	No	No
Auto-scale out	Yes	Yes	Yes	Yes	Yes	Yes
Routed	Yes	Yes	Yes	Yes	Yes	Yes
Transparent	No	No	No	No	No	No
WCCP	No	No	No	No	No	No
Static and Policy Based Routing	Yes	Yes	Yes	Yes	Yes	Yes
OSPF					No	No
BGP	Yes	Yes	Yes	Yes	Yes	Yes
RIP					No	
EIGRP					No	
IS-IS					No	
Multicast	No	No	No	No	No	
NAT/PAT	Yes	Yes	Yes	Yes	Only Outbound SNAT & Inbound DNAT. DNAT not supported in Spoke to Spoke environments.	Only Outbound SNAT & Inbound DNAT. DNAT not supported in Spoke to Spoke environments.
Platform Exchange Grid (pxGrid)	Yes	Yes	No	No	No	No
Device APIs	Yes	Yes	Yes	Yes	Yes	Yes
AAA for Management						
TACACS	No	No	Yes	Yes	No	No
Radius	Yes	Yes	Yes	Yes	No	No
SAML	Yes	Yes	Yes	Yes	No	No
MFA-RSA SDI					No	No
MFA-Duo	Yes	Yes	Yes	Yes	No	No
Local Auth	Yes	Yes	Yes	Yes	Yes	Yes
RBAC	Yes	Yes	Yes	Yes	Yes	Yes

Security Features	FTD 7.3 in Azure	FTD 7.2 in Azure	ASA 9.19 in Azure	ASA 9.18 in Azure	Azure Firewall	Azure Firewall Premium
Management Platform						
On-box	Yes	Yes	Yes	Yes	Not applicable	Not applicable
Cloud delivered	Yes	Yes	Yes	Yes	Yes	Yes
Centralized	Yes	Yes	Yes	Yes	Yes	Yes
Single Sign On (SSO)	Yes	Yes	Yes	Yes	Yes	Yes
Upgrade	Yes	Yes	Yes	Yes	Not applicable	Not applicable
Backup/Restore	Yes	Yes	Yes	Yes	Yes	Yes
Health Policy and Monitoring	Yes	Yes	Yes	Yes	Yes	Yes
Policy Inheritance	Yes	Yes	Yes	Yes	No	No
Audit	Yes	Yes	Yes	Yes	Yes	Yes
Change Control	Yes	Yes	Yes	Yes	Yes	Yes
Multi-domain management	Yes	Yes	Yes	Yes	No	No
Azure Application Insights	Yes	Yes	No	No	Yes	Yes

Security Features	FTD 7.3 in Azure	FTD 7.2 in Azure	ASA 9.19 in Azure	ASA 9.18 in Azure	Azure Firewall	Azure Firewall Premium
Management Platform						
Enterprise Firewall	Included	Included	Included	Included	Free to use. Deployment and Data processing cost	Free to use. Deployment and Data processing cost
Application Visibility	Included	Included	NA	NA	Free to use. Deployment and Data processing cost	Free to use. Deployment and Data processing cost
IPS	BYOL Smart Licensing	BYOL Smart Licensing	NA	NA	Not applicable	Not applicable
Malware Remediation	BYOL Smart Licensing	BYOL Smart Licensing	NA	NA	Not applicable	Not applicable
Malware Sandboxing	BYOL Smart Licensing	BYOL Smart Licensing	NA	NA	Not applicable	Not applicable
URL Filtering	BYOL Smart Licensing	BYOL Smart Licensing	NA	NA	Free to use. Deployment and Data processing cost	Free to use. Deployment and Data processing cost
Management Cloud Delivered	BYOL Smart Licensing (Cisco Defense Orchestrator is supported but CDO licensing is separate)	BYOL Smart Licensing (Cisco Defense Orchestrator is supported but CDO licensing is separate)	BYOL Smart Licensing (Cisco Defense Orchestrator is supported but CDO licensing is separate)	BYOL Smart Licensing ((Cisco Defense Orchestrator is supported but CDO licensing is separate)	Additional Service to install. Free to use. Deployment and Data processing cost	Additional Service to install. Free to use. Deployment and Data processing cost
Management Centralized	BYOL Smart Licensing (Firepower Management Center is supported but FMC licensing is separate)	BYOL Smart Licensing (Firepower Management Center is supported but FMC licensing is separate)	BYOL Smart Licensing (CSM is supported but CSM licensing is separate)	BYOL Smart Licensing (CSM is supported but CSM licensing is separate)	Additional Service to install. Free to use. Deployment and Data processing cost	Additional Service to install. Free to use. Deployment and Data processing cost
Management On-box	Included (FDM)	Included (FDM)	Included (ASDM)	Included (ASDM)	Included	Included

Security Features	FTD 7.3 in Azure	FTD 7.2 in Azure	ASA 9.19 in Azure	ASA 9.18 in Azure	Azure Firewall	Azure Firewall Premium
Deployment						
Total # of NICs	Up to 8	Up to 8	Up to 8	Up to 8	Not applicable	Not applicable
Azure Instances	Standard_D3, Standard_D3_v2, Standard_D4_v2, Standard_D5_v2 Standard_D8s_v3 Standard_D16s_v3 Standard_F8s_v2 Standard_F16s_v2	Standard_D3, Standard_D3_v2, Standard_D4_v2, Standard_D5_v2 Standard_D8s_v3 Standard_D16s_v3 Standard_F8s_v2 Standard_F16s_v2	Standard_D3, Standard_D4, Standard_D5. Standard_D3_v2, Standard_D4_v2, Standard_D5_v2, Standard_D8_v3, Standard_DS3, Standard_DS4, Standard_DS5, Standard_DS3_v2, Standard_DS4_v2, Standard_DS5_v2 Standard_F4, Standard_F8, Standard_F16, Standard_F4s, Standard_F8s, Standard_F16s Standard_D8s_v3 Standard_D16s_v3 Standard_F8s_v2 Standard_F16s_v2	Standard_D3, Standard_D4, Standard_D5. Standard_D3_v2, Standard_D4_v2, Standard_D5_v2, Standard_D8_v3, Standard_DS3, Standard_DS4, Standard_DS5, Standard_DS3_v2, Standard_DS4_v2, Standard_DS5_v2 Standard_F4, Standard_F8, Standard_F16, Standard_F4s, Standard_F8s, Standard_F16s Standard_D8s_v3 Standard_D16s_v3 Standard_F8s_v2 Standard_F16s_v2	Not applicable	Not applicable
Azure Security Center	Yes	Yes	Yes	Yes	Yes	Yes
Azure Government Cloud	Yes	Yes	Yes	Yes	Yes	Yes
Custom Image Snapshot	Yes	Yes	No	No	Yes	Yes

Public Cloud Secure Firewall

Google Cloud vs. Cisco Secure Firewall

LEGEND
Supported (Yes)
Partial
Not supported (No)

Security Features	FTD 7.3 in Google Cloud	ASA 9.19 in Google Cloud	Google Cloud Firewall
Site to Site VPN			
IPSec / Site to Site VPN - Hub & Spoke	Yes	Yes	Using VPN
IPSec / Site to Site VPN - 3rd party / Extranet	Yes	Yes	Using VPN
PKI support	Yes	Yes	Using VPN
VTI support	Yes	Yes	Using VPN
IKEv2 support	Yes	Yes	Using VPN
RA VPN			
Clientless-SSL VPN	No	Yes	No
Anyconnect or Client VPN	Yes	Yes	No
SAML	Yes	Yes	No
MFA-RSA SDI	Yes	Yes	No
MFA-Duo	Yes	Yes	No
Local Auth	Yes	Yes	Yes
RADIUS	Yes	Yes	No
TACACS	No	Yes	No
Dynamic Access Policy	Yes	Yes	

Security Features	FTD 7.3 in Google Cloud	ASA 9.19 in Google Cloud	Google Cloud Firewall
Enterprise FW	Yes	Yes	Yes
App Visibility & Control	Yes		
Geolocation	Yes	No	No
SSL Decryption	Yes	No	
Known key	Yes	No	No
Resign	Yes	No	No
NGIPS / NGIDS	Yes	No	No
Snort 3	Yes	No	No
DDoS	No	No	
URL/Web Filtering	Yes	No	
Web Proxy Integration	No	No	No
Advance Malware Protection and Breach Detection	Yes	No	No
Continuous Analysis & Retrospective Detection	Yes	No	No
Malware Remediation	Yes	No	No
Integrated Sandboxing	Yes	No	No
Contextual Awareness (who, what, when, where, why, How)	Yes	No	No
User Awareness	Yes	Yes	No
Security Automation & Adaptive Threat Management	Yes	No	Yes
IoCs	Yes	No	No
Network Awareness	Yes	No	No
Endpoint Awareness	Yes	No	No
Network File Trajectory	Yes	No	No
Impact Assesment	Yes	No	No
DNS Based Policy & Sinkholing	Yes	No	
Encrypted Traffic Analytics	Yes	Yes	

Security Features	FTD 7.3 in Google Cloud	ASA 9.19 in Google Cloud	Google Cloud Firewall
Threat Intelligence			
System Feed (Talos or eq)	Yes	No	Yes
3rd party – system feed	Yes	No	No
3rd party feeds /Threat Intelligence Director / Integrations	Yes	No	
Automated Intelligence feeds	Yes	No	
Operational Capabilities			
Software Defined Segmentation	No	No	Yes
Automatic Threat Containment	Yes	No	
Syslog & Event Data Export			
Local / Built into management	Yes	Yes	Yes
Syslog	Yes	Yes	Yes
Reporting Dashboards	Yes	Yes	Yes
SIEM	Yes	Yes	Yes
SOAR	Yes – Based on Vendor support **	Yes – Based on Vendor support **	Yes
Cisco Threat Response	Yes	No	No
SecureX	Yes	No	No
Remediation API	Yes	No	No
Host API	Yes	No	No

Security Features	FTD 7.3 in Google Cloud	ASA 9.19 in Google Cloud	Google Cloud Firewall
NetOps Features			
High Availability			Yes
Clustering	Yes		No
Auto-scale out		Yes	Yes
Routed	Yes	Yes	Yes
Transparent	No	No	No
WCCP - On -USECASE	No	No	No
Static and Policy Based Routing	Yes	Yes	Yes
OSPF			No
BGP	Yes - Anything with Unicast	Yes	Yes
RIP			No
EIGRP			No
IS-IS			No
Multicast	No	No	No
NAT/PAT	Yes	Yes	
Platform Exchange Grid (pxGrid)		No	No
Device APIs	Yes	Yes	Yes
AAA for Management			
TACACS	No	Yes	No
Radius	Yes	Yes	No
SAML	Yes	Yes	No
MFA-RSA SDI			No
MFA-Duo	Yes	Yes	No
Local Auth	Yes	Yes	Yes
RBAC	Yes	No	Yes

Security Features	FTD 7.3 in Google Cloud	ASA 9.19 in Google Cloud	Google Cloud Firewall
Management Platform			
On-box	Yes	Yes	NA
Cloud delivered	Yes	Yes	Yes
Centralized	Yes	Yes	Yes
Single Sign On (SSO)	Yes	Yes (CDO)	Yes
Upgrade	Yes	Yes	NA
Backup/Restore	Yes	Yes	Yes
Health Policy and Monitoring	Yes	Yes	Yes
Policy Inheritance	Yes	Yes	No
Audit	Yes	Yes	Yes
Change Control	Yes	Yes	Yes
Multi-domain management	Yes -Through FMC	No	No
Enterprise Firewall	Included	Included	Free to use. Deployment and Data processing cost
Application Visibility	Included	NA	Free to use. Deployment and Data processing cost
IPS	BYOL Smart Licensing	NA	NA
Malware Remediation	BYOL Smart Licensing	NA	NA
Malware Sandboxing	BYOL Smart Licensing	NA	NA
URL Filtering	BYOL Smart Licensing	NA	Free to use. Deployment and Data processing cost
Management Cloud Delivered	Yes	BYOL Smart Licensing (Cisco Defense Orchestrator is supported but CDO licensing is separate)	Additional Service to install. Free to use. Deployment and Data processing cost
Management Centralized	BYOL Smart Licensing (Firepower Management Center is supported but FMC licensing is separate)	BYOL Smart Licensing (CSM is supported but CSM licensing is separate)	Additional Service to install. Free to use. Deployment and Data processing cost
Management On-box	Included	Included	Included

Security Features	FTD 7.3 in Google Cloud	ASA 9.19 in Google Cloud	Google Cloud Firewall
Deployment			
Total # of NICs	Based on Instance (Datasheet)	Based on Instance (Datasheet)	NA
Google Instances	FTDv GCP N2-Standard-4 FTDv GCP N2-Standard-8 FTDv GCP N2-Standard-16 FTDv GCP C2-Standard-4 FTDv GCP C2-Standard-8 FTDv GCP C2-Standard-16 FTDv GCP N2-highcpu-16 FTDv GCP N2-highmem-16	ASAv GCP N2-Standard-4 ASAv GCP N2-Standard-8 ASAv GCP N2-Standard-16 ASAv GCP C2-Standard-4 ASAv GCP C2-Standard-8 ASAv GCP C2-Standard-16 ASAv GCP N2-highcpu-16 ASAv GCP N2-highmem-16	NA
Autoscale	Yes	No	NA
Google Security Centre	No	No	Yes
Google Government Cloud	No	No	Yes

Public Cloud Secure Firewall

AWS Firewall vs. Cisco Secure Firewall

LEGEND
Supported (Yes)
Partial
Not supported (No)

Security Features	FTD 7.3 in AWS	ASA 9.19 in AWS	AWS Firewall
Site to Site VPN			
IPSec / Site to Site VPN - Hub & Spoke	Yes	Yes	Using VPN
IPSec / Site to Site VPN - 3rd party / Extranet	Yes	Yes	Using VPN
PKI support	Yes	Yes	Using VPN
VTI support	Yes	Yes	Using VPN
IKEv2 support	Yes	Yes	Using VPN
RA VPN			
Clientless-SSL VPN	No	Yes	No
Anyconnect or Client VPN	Yes	Yes	Yes
SAML	Yes	Yes	Yes
MFA-RSA SDI	Yes	Yes	No
MFA-Duo	Yes	Yes	No
Local Auth	Yes	Yes	Yes
RADIUS	Yes	Yes	No
TACACS	No	Yes	No
Dynamic Access Policy	Yes	Yes	No

Security Features	FTD 7.3 in AWS	ASA 9.19 in AWS	AWS Firewall
Enterprise FW	Yes	Yes	Yes
App Visibility & Control	Yes		
Geolocation	Yes	No	No
SSL Decryption	Yes	No	
Known key	Yes	No	No
Resign	Yes	No	No
NGIPS / NGIDS	Yes	No	No
Snort 3	Yes	No	No
DDoS	No	No	
URL/Web Filtering	Yes	No	
Web Proxy Integration	No	No	No
Advance Malware Protection and Breach Detection	Yes	No	No
Continuous Analysis & Retrospective Detection	Yes	No	No
Malware Remediation	Yes	No	No
Integrated Sandboxing	Yes	No	No
Contextual Awareness (who, what, when, where, why, How)	Yes	No	No
User Awareness	Yes	Yes	No
Security Automation & Adaptive Threat Management	Yes	No	Yes
IoCs	Yes	No	No
Network Awareness	Yes	No	No
Endpoint Awareness	Yes	No	No
Network File Trajectory	Yes	No	No
Impact Assesment	Yes	No	No
DNS Based Policy & Sinkholing	Yes	No	
Encrypted Traffic Analytics	Yes	Yes	

Security Features	FTD 7.3 in AWS	ASA 9.19 in AWS	AWS Firewall
Threat Intelligence			
System Feed (Talos or eq)	Yes	No	Yes
3rd party – system feed	Yes	No	No
3rd party feeds /Threat Intelligence Director / Integrations	Yes	No	
Automated Intelligence feeds	Yes	No	
Operational Capabilities			
Software Defined Segmentation	No	No	Yes
Automatic Threat Containment	Yes	No	
Syslog & Event Data Export			
Local / Built into management	Yes	Yes	Yes
Syslog	Yes	Yes	Yes
Reporting Dashboards	Yes	Yes	Yes
SIEM	Yes	Yes	Yes
SOAR	Yes – Based on Vendor support **	Yes – Based on Vendor support **	Yes
Cisco Threat Response	Yes	No	No
SecureX	Yes	No	No
Remediation API	Yes	No	No
Host API	Yes	No	No

Security Features	FTD 7.3 in AWS	ASA 9.19 in AWS	AWS Firewall
NetOps Features			
High Availability	No		Yes
Clustering	Yes	Yes	No
Auto-scale out		Yes	Yes
Routed	Yes	Yes	Yes
Transparent	No	No	No
WCCP - On -USECASE	No	No	No
Static and Policy Based Routing	Yes	Yes	Yes
OSPF	Yes	Yes	No
BGP	Yes - Anything with Unicast	Yes	Yes
RIP	Yes	Yes	No
EIGRP	Yes	Yes	No
IS-IS			No
Multicast	No	No	No
NAT/PAT	Yes	Yes	
Platform Exchange Grid (pxGrid)	Yes	No	No
Device APIs	Yes	Yes	Yes
AAA for Management			
TACACS	No	Yes	No
Radius	Yes	Yes	No
SAML	Yes	Yes	Yes
MFA-RSA SDI			No
MFA-Duo	Yes	Yes	No
Local Auth	Yes	Yes	Yes
RBAC	Yes	No	Yes

Security Features	FTD 7.3 in AWS	ASA 9.19 in AWS	AWS Firewall
Management Platform			
On-box	Yes	Yes	Not applicable
Cloud delivered	Yes	Yes	Yes
Centralized	Yes	Yes	Yes
Single Sign On (SSO)	Yes	Yes (CDO)	Yes
Upgrade	Yes	Yes	Not applicable
Backup/Restore	Yes	Yes	Yes
Health Policy and Monitoring	Yes	Yes	Yes
Policy Inheritance	Yes	Yes	No
Audit	Yes	Yes	Yes
Change Control	Yes	Yes	Yes
Multi-domain management	Yes -Through FMC	No	No
Enterprise Firewall	Included	Included	Free to use. Deployment and Data processing cost
Application Visibility	Included	NA	Free to use. Deployment and Data processing cost
IPS	BYOL Smart Licensing	NA	Basic IPS functions with Suricata based IPS rules
Malware Remediation	BYOL Smart Licensing	NA	No
Malware Sandboxing	BYOL Smart Licensing	NA	No
URL Filtering	BYOL Smart Licensing	NA	Free to use. Deployment and Data processing cost
Management Cloud Delivered	Yes	BYOL Smart Licensing (Cisco Defense Orchestrator is supported but CDO licensing is separate)	Additional Service to install. Free to use. Deployment and Data processing cost
Management Centralized	BYOL Smart Licensing (Firepower Management Center is supported but FMC licensing is separate)	BYOL Smart Licensing (CSM is supported but CSM licensing is separate)	Additional Service to install. Free to use. Deployment and Data processing cost
Management On-box	Included	Included	Included

Security Features	FTD 7.3 in AWS	ASA 9.19 in AWS	AWS Firewall
Deployment			
Total # of NICs	Based on Instance (Datasheet)	Based on Instance (Datasheet)	NA
AWS Instances	AWS Instance Types	AWS Instance Types	NA
Autoscale	Yes	Yes	NA
AWS Guard Duty	Yes	No	Yes
AWS Government Cloud	Yes	Yes	Yes
Custom Image Snapshot	Custom Image Snapshot		N/A