

TECHNICAL REFERENCE, SANITISED VERSION

Perimeter Firewall and Management Center

Cisco Secure Firewall 3105 HA Pair and Cisco Secure Firewall Management Center, documented from a device backup and a management centre backup. The organisation is not named and every identifying name, address and custom port has been substituted; the rules and their structure are unchanged.

Device FW3105-1

Platform Cisco Secure Firewall 3105, FTD 7.6.4

Manager Firepower Management Center

Source device backup, configuration only

Version Sanitised for external reading

Online wright.solanderpartners.com

1 Introduction

This document describes the perimeter firewall of Y corp: a Cisco Secure Firewall 3105 high availability pair running Firewall Threat Defense (FTD), managed by a Cisco Secure Firewall Management Center (FMC). It documents the configuration as it stands, with the names and values held in the FMC.

SOURCE	TAKEN	CONTENT
FTD device backup, FW3105-1 (primary)	2026-09-12 16:00 UTC	device configuration, FXOS configuration, deployed policy files
FMC configuration backup, fmc93	2026-09-14 02:00 UTC	FMC database (policies, objects, platform settings, VPN), FMC system files
Last policy deployment	2026-09-10 08:52 UTC	configuration version compiled on the device

Conventions used in this document:

- Object, policy, zone and interface names are written as they appear in the FMC, including their original spelling, except where a value has been substituted for this version (below).
- Where one FMC rule compiles into several device lines, the FMC rule is documented and the device line count is given.
- Pre-shared keys, SNMP community strings, SNMPv3 credentials and passwords are present in the configuration and are not reproduced.
- Personal user accounts are written as role labels, Y-1 to Y-6 for the organisation and X-1 to X-5 for the integrator.

This is a real document, produced from a live production firewall, published with the identity of the organisation removed. Every rule, object, count and design decision is as the device holds it; only the values that would identify the organisation or its partners have been replaced: the names of servers, sites, networks, applications and partners, serial numbers, every address, the port numbers that are not a standard default, and anything that places it in a country. Public addresses therefore appear as placeholders from 240.0.0.0/4, a reserved range that is never routed, and private addresses as other private addresses. The full account is at the end, under *About this version*.

1.1 DOCUMENT STRUCTURE

CHAPTER	CONTENT
2 Physical Architecture	components, the HA pair, the FMC, the internal firewall, port assignment
3 Network Design and Firewall Configuration	management, high availability, interfaces, routing, IP address space
4 Access Control and NAT	objects, zones, access control policy grouped by function, NAT
5 Site to Site VPN	IKE and IPsec proposals and policies, route based and policy based tunnels
6 FTD Platform Settings, Management, Logging and Monitoring	SNMP, syslog, time synchronisation
7 FMC System Management	FMC system configuration, user roles and users
8 Configuration Backup	scheduled backups and tasks
Appendix A	every network object referenced by rules, NAT, VPN and routing, grouped by function, with its value
Appendix B	every port object referenced by rules and NAT, with its value
About this version	what was substituted for publication, and what was not

2 Physical Architecture

2.1 DESIGN RATIONALE, TWO LAYER FIREWALL ARCHITECTURE

The two layer design replaced a single layer Fortinet FortiGate 600E HA pair. Two firewalls from two vendors now stand in line:

- Perimeter layer, Cisco Secure Firewall 3105 HA pair (this document): Internet connection, site to site VPNs, the Google Partner Interconnect, the DMZs, and destination NAT of the VPN_access service ports to the internal firewall.
- Internal layer, Fortinet FortiGate HA pair: default gateway of every internal VLAN, the only VPN_access remote access VPN termination, and the policy point for user and server traffic.

The two layers are joined by a routed transit network (TRANSIT, VLAN 310) carried by the Cisco Catalyst 9500 core, which works at layer 2 between them. Traffic from the Internet to an internal segment passes both firewalls. The migration left two traces in this configuration: TEMPTRANSIT, the "temporary p2p link to Fortinet 600", and 87 access rules commented "copied from Fortinet_Migrated_Policy".

2.2 ARCHITECTURE OVERVIEW

COMPONENT	MODEL	SOFTWARE	ROLE
FTD-HQ-HA	Cisco Secure Firewall 3105, 2 units	FTD 7.6.4 (build 69)	perimeter firewall, active/standby
fmc93	FMCv for VMware (FS-VMW-SW-K9)	FMC 7.6.5 (build 106)	management of the FTD pair
Fortinet-transit	Fortinet FortiGate, 2 units	FortiOS	internal firewall, active/passive
core9500	Cisco Catalyst 9500 stack	not in these backups	collapsed core, layer 2 between the firewalls; Port-channel1, 802.1Q

2.3 PERIMETER FIREWALL, CISCO SECURE FIREWALL 3105 HA PAIR

UNIT	HA ROLE	STATE AT BACKUP	SERIAL	MANAGEMENT IP	MANAGEMENT MAC
FW3105-1	Primary	Active	withheld	10.147.50.21/24	4C:01:F7:xx:xx:xx
FW3105-2	Secondary	Standby Ready	withheld	10.147.50.199/24	4C:01:F7:xx:xx:xx
ITEM	VALUE				
HA group (FMC)	FTD-HQ-HA, active/standby				
Hardware	FPR-3105, 24 cores, 16 GB, network module slot 1: 8 x 1G RJ45 + 8 x 10G SFP				
Firewall mode	routed, single context, VRF Global only				
Software	FTD 7.6.4 build 69; ASA/LINA 9.22(2)29; FXOS 2.16(1.147); Snort 3.1.79.400-43				
Content versions	VDB 408; LSP lsp-rel-20260902-2004; intrusion rule update 2026-09-09-001-vrt; geolocation 2026-08-15-093				
Licences	Essentials (BASE), IPS (THREAT), Malware Defense (MALWARE), URL Filtering (URLFilter)				
Software history	7.3.1-19 installed 2025-04-05; 7.4.2-172 2025-05-26; 7.4.2.3 2025-08-20; 7.4.2.4 2025-10-01; 7.6.2 and 7.6.2.1 2025-12-20; 7.6.4-69 2026-03-09				

2.4 PERIMETER FIREWALL, MANAGEMENT SYSTEM CISCO SECURE FIREWALL MANAGEMENT CENTER

ITEM	VALUE
Host name	fmc93.example.com
Model	Cisco Secure Firewall Management Center for VMware (FMCv), product ID FS-VMW-SW-K9
Software	7.6.5 (build 106), hotfix CY-2 applied 2026-09-08
Memory	32 GB
Management interface	eth0 10.147.50.139/24, gateway 10.147.50.65, MAC 00:50:56:xx:xx:xx
Managed devices	FW3105-1, FW3105-2 (HA group FTD-HQ-HA)
Device channel	sftunnel TCP/8305, TLS 1.2 to 1.3, heartbeat 120 s
Smart Licensing	registered 2025-05-19, authorisation renewed 2026-09-08
Software history	7.4.2 installed 2025-05-16; 7.4.2.2 2025-05-19; 7.4.2.3 2025-08-20; 7.4.2.4 2025-10-01; 7.6.2 and 7.6.2.1 2025-12-20; 7.6.5 2026-03-09; hotfix CY-2 2026-09-08
Malware cloud	AMP EU cloud (cloud-sa.eu.amp.cisco.com)

2.5 INTERNAL FIREWALL, FORTINET FORTIGATE HA PAIR

ITEM	VALUE (FROM THE INTERNAL FIREWALL REFERENCE DOCUMENT)
Model	Fortinet FortiGate, 2 units, HA active/passive, HA group 10
Software	FortiOS
HA links	two heartbeat links (1G RJ45), one session synchronisation link (10G SFP+)
Uplink	one LACP aggregate, 2 x 10G, to the Catalyst 9500; carries all internal VLANs and the transit to the FTD; loss of either member fails over to the passive unit
Role	default gateway of the internal VLANs; VPN_access services (Corporate, Admin, Partner, UAT)

The FortiGate pair is not managed by the FMC and is not in these backups. On the FTD it is defined as follows:

FMC OBJECT / SETTING	VALUE	USE ON THE FTD
Fortinet-transit	10.243.31.246	next hop on TRANSIT for RFC 1918 space and the internal networks
TRANSIT (Port-channel1.310)	10.243.31.242/29	interface description: "p2p connection to Fortinet"
Fortinet_Loopbacks	100.91.136.0/24	routed to Fortinet-transit
Fortinet_Loopback1	100.91.136.50	NAT (4.4) and access rules (4.3.1)
Fortinet_Loopback2	100.91.136.197	NAT (4.4) and access rules (4.3.1)
Fortinet_Loopback3	100.91.136.221	NAT (4.4) and access rules (4.3.1)
Fortinet_Loopback4	100.91.136.183	access rules (4.3.1)
Fortinet_Loopback7	100.91.136.104	NAT (4.4) and access rules (4.3.1)
Fortinet_Loopback8	100.91.136.193	NAT (4.4) and access rules (4.3.1)
Fortinet_Loopback9	100.91.136.236	NAT (4.4) and access rules (4.3.1)

2.6 PHYSICAL PORT ASSIGNMENT, CISCO SECURE FIREWALL 3105 HA PAIR

Port settings are from the FXOS configuration of the primary unit; both units are cabled the same way.

PORT	MEDIA	ADMIN STATE	SPEED	LOGICAL INTERFACE	CONNECTION
Ethernet1/1	RJ45	enabled	1 Gbps full, autonegotiation off	outside	Internet (ISP), LLDP receive only
Ethernet1/2	RJ45	enabled	1 Gbps full, autonegotiation on	DMZ_EXTFW	EXT firewall (Fortinet), LLDP send and receive
Ethernet1/3	RJ45	enabled	1 Gbps full, autonegotiation off	Google_IC	Google Partner Interconnect, MTU 1460
Ethernet1/4 to 1/8	RJ45	disabled			
Ethernet1/9	SFP+, 3 m 10G copper DAC	enabled	10 Gbps	Port-channel1	LACP active, to core9500
Ethernet1/10	SFP+, 3 m 10G copper DAC	enabled	10 Gbps	Port-channel1	LACP active, to core9500
Ethernet1/11 to 1/15	SFP+, empty	disabled			
Ethernet1/16	SFP+, 3 m 10G copper DAC	enabled	10 Gbps	HA-LINK	failover and state link to the peer unit
Management1/1	RJ45	enabled		management	management-only, 10.147.50.0/24

3 Network Design and Firewall Configuration

3.1 DEVICE MANAGEMENT (FTD)

ITEM	PRIMARY	SECONDARY
Management interface	management0 10.147.50.21/24	management0 10.147.50.199/24
Default gateway	10.147.50.65	10.147.50.65
Manager	FMC 10.147.50.139, sftunnel TCP/8305	FMC 10.147.50.139, sftunnel TCP/8305
Management DNS	208.67.222.222, 208.67.220.220, 2620:119:35::35	same
Management NTP	127.0.0.2 (the FMC, through sftunnel), local clock as fallback	same
Management access (host firewall)	TCP/22 SSH, TCP/8305 sftunnel, ICMP echo; UDP/161 only from 10.243.31.4	same
SSH	root login off, 3 attempts, 1 session, no forwarding; SHA-2 MACs; AES-GCM, ChaCha20, AES-CTR	same

Data plane DNS (platform settings): server group Internal-DNS-servers = 10.243.31.65, 10.243.31.93, domain example.com, used for FQDN objects, lookups through the management interface.

3.1.1 High Availability Configuration

SETTING	VALUE
Failover	enabled, active/standby, FW3105-1 = primary
Failover link	HA-LINK on Ethernet1/16
Stateful failover link	HA-LINK on Ethernet1/16 (shared with the failover link)
Addresses	169.254.68.214/24 (primary) / 169.254.68.141/24 (secondary)
State replication	HTTP replication on
Unit poll / hold	1 s / 15 s
Interface poll / hold	5 s / 25 s
Interface policy	failover after 1 failed monitored interface
Failover key	not set in the FMC HA settings

Interface monitoring as set in the FMC HA settings; the device carries the same (no monitor-interface for TEMPTRANSIT and DMZ_EXTFW). No standby IP address is configured on the data interfaces.

INTERFACE	ACTIVE IP	MONITORED
core9500		yes
TRANSIT	10.243.31.242/29	yes
DMZ_IDP	10.230.134.87/24	yes
TEMPTRANSIT	10.243.31.252/29	no
management		yes

INTERFACE	ACTIVE IP	MONITORED
Google_IC	169.254.127.194/29	yes
outside	247.222.237.1/29	yes
SiteN_vti	169.254.253.242/30	yes
SiteT_New_vti	169.254.130.26/30	yes
Google_IC_local	169.254.12.85/30	yes
DMZ_EXTFW	10.243.31.183/28	no

3.1.2 Interfaces

INTERFACE	NAME	VLAN	IPv4	MTU	SECURITY ZONE	INTERFACE GROUP	DESCRIPTION
Port-channel1	core9500		no IP	1500			
Port-channel1.310	TRANSIT	310	10.243.31.242/29	1500	INSIDE-ZONE	Transit_IG	p2p connection to Fortinet
Port-channel1.311	TEMPTRANSIT	311	10.243.31.252/29	1500	INSIDE-ZONE		temporary p2p link to Fortinet 600
Port-channel1.320	DMZ_IDP	320	10.230.134.87/24	1500	DMZ_IDP		IDP DMZ
Ethernet1/1	outside		247.222.237.1/29	1500	OUTSIDE-ZONE		
Ethernet1/2	DMZ_EXTFW		10.243.31.183/28	1500	DMZ_EXTFW		EXTFW Fortinet
Ethernet1/3	Google_IC		169.254.127.194/29	1460	GIC		Google Partner Interconnect
Management1/1	management		no IP	1500			management-only

All data interfaces have security level 0 (the FMC does not use security levels; access is by zone). IPv6 is not configured on any interface. Ethernet1/4 to 1/8 and 1/11 to 1/15 are shut down.

INTERFACE	SETTING	VALUE
Unicast RPF (reverse path check)	TRANSIT, TEMPTRANSIT, outside	
ICMP to the device	echo permitted on TRANSIT, TEMPTRANSIT, outside; echo-reply denied on the same three; time-exceeded and unreachable denied on outside; unreachable rate limit 1, burst 1	
Path monitoring	outside, monitors 247.222.237.4 (policy-route path-monitoring)	

3.1.3 Default, Static and Dynamic Routing

Static routes as defined in the FMC, with the device routes they compile to:

INTERFACE	NETWORKS (FMC OBJECT, VALUE)	GATEWAY	METRIC
outside	any-ipv4 (0.0.0.0/0)	isp-wan-gw (247.222.237.4)	1
TRANSIT	IPv4-Private-All-RFC1918 (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16); Fortinet_Loopbacks (100.91.136.0/24)	Fortinet-transit (10.243.31.246)	1
DMZ_EXTFW	PARTNER-EXT-FW_Loopback (245.141.92.205)	PARTNER-EXT-FW_Address (10.243.31.186)	1
outside	PARTNER_Public_Services (245.88.176.0/23, 245.88.200.228, 246.121.155.26, 247.196.136.228)	isp-wan-gw (247.222.237.4)	1
SiteN_vti	SiteN_S2SRemote (10.75.51.0/24)	169.254.253.241	1
SiteT_New_vti	SiteT_S2SRemote (10.94.108.0/24, 10.243.158.0/24, 10.136.41.0/24, 172.16.78.0/24)	169.254.130.25	1

INTERFACE	NETWORKS (FMC OBJECT, VALUE)	GATEWAY	METRIC
TRANSIT	Tango (10.243.31.0/25); static_remote_SiteM_ESXI-MGMT (10.180.162.0/24); static_remote_Test_vMotion (10.154.21.0/24); SiteM_vMotion (10.114.102.0/24); SiteM_ESXI-GCE-Uplink (10.229.126.0/24)	Fortinet-transit (10.243.31.246)	1

The 7 FMC routes compile to 20 device routes (network groups expand to one route each):

INTERFACE	DESTINATION	NEXT HOP	METRIC
outside	0.0.0.0/0	247.222.237.4	1
TRANSIT	10.0.0.0/8	10.243.31.246	1
TRANSIT	10.243.31.0/25	10.243.31.246	1
TRANSIT	10.180.162.0/24	10.243.31.246	1
TRANSIT	10.114.102.0/24	10.243.31.246	1
TRANSIT	10.229.126.0/24	10.243.31.246	1
TRANSIT	10.154.21.0/24	10.243.31.246	1
SiteT_New_vti	10.136.41.0/24	169.254.130.25	1
SiteT_New_vti	10.243.158.0/24	169.254.130.25	1
SiteT_New_vti	10.94.108.0/24	169.254.130.25	1
SiteN_vti	10.75.51.0/24	169.254.253.241	1
outside	246.121.155.26/32	247.222.237.4	1
outside	247.196.136.228/32	247.222.237.4	1
TRANSIT	100.91.136.0/24	10.243.31.246	1
DMZ_EXTFW	245.141.92.205/32	10.243.31.186	1
TRANSIT	172.16.0.0/12	10.243.31.246	1
SiteT_New_vti	172.16.78.0/24	169.254.130.25	1
outside	245.88.200.228/32	247.222.237.4	1
outside	245.88.176.0/23	247.222.237.4	1
TRANSIT	192.168.0.0/16	10.243.31.246	1

Dynamic routing, BGP (towards Google Cloud over the Partner Interconnect):

SETTING	VALUE
Local AS	64513
Router ID	169.254.127.194
Timers (keepalive / hold)	20 s / 60 s
Graceful restart	on, restart time 1 s
Path selection	always-compare-med, deterministic-med
Log neighbour changes	on
Path MTU discovery	disabled on both neighbours

SETTING	VALUE
Advertised networks	10.180.162.0/24, 10.114.102.0/24, 10.229.126.0/24, 10.154.21.0/24, 10.243.31.0/25 (FMC objects Tango, static_remote_SiteM_ESXI-MGMT, static_remote_Test_vMotion, SiteM_vMotion, SiteM_ESXI-GCE-Uplink)

NEIGHBOUR	REMOTE AS	INBOUND FILTER	OUTBOUND FILTER	OUTBOUND ROUTE MAP	OPTIONS
169.254.12.86	16550	GooGle_IC_incoming	Google_IC_outgoing	TO_GCP_OUT	HA graceful restart off
169.254.127.193	16550	GooGle_IC_incoming	Google_IC_outgoing	TO_GCP_OUT_Prefer	BFD multi-hop; HA graceful restart

FILTER	TYPE	PERMITS
GooGle_IC_incoming	standard ACL, routes accepted from Google	10.190.80.0/22, 10.231.244.0/22, 35.199.192.0/19, 10.135.44.0/24
Google_IC_outgoing	standard ACL, routes sent to Google	10.243.31.0/25, 10.180.162.0/24, 10.154.21.0/24, 10.114.102.0/24, 10.229.126.0/24
To_GCP	prefix list	10.180.162.0/24
To_GCP2	prefix list	10.243.31.0/25, 10.154.21.0/24
To_GCP3	prefix list	10.114.102.0/24, 10.229.126.0/24
TO_GCP_OUT	route map, seq 10	match To_GCP2, To_GCP; set metric 1000, metric-type internal
TO_GCP_OUT_Prefer	route map, seq 1	match To_GCP2, To_GCP, To_GCP3; set metric 500, metric-type internal

3.2 IP ADDRESS SPACE OVERVIEW, EXTERNAL AND SITE TO SITE VPN TUNNEL INTERFACES

The Internet connection is 247.222.237.1/29 on outside. The public /29 is used as follows:

ADDRESS	FMC OBJECTS	USE
247.222.237.4	isp-wan-gw	ISP gateway (default route next hop)
247.222.237.2	Public_IP_4	NAT publication, section 4.4
247.222.237.5	Public_IP_2, mail.example.com-HTTP	NAT publication, section 4.4
247.222.237.1	FortinetVPN, public_1	outside interface address; VPN endpoint; PAT address
247.222.237.6	Public_IP_3	NAT publication, section 4.4
247.222.237.3	IDP-PUBLIC	IDP publication (NAT)

Route based VPN tunnel interfaces (static VTI, IPsec, source outside):

INTERFACE	NAME	TUNNEL IP	PEER (TUNNEL DESTINATION)	IPSEC PROFILE	SECURITY ZONE
Tunnel1	Google_IC_local	169.254.12.85/30	245.78.19.66	FMC_IPSEC_PROFILE_1	GIC
Tunnel2	SiteN_vti	169.254.253.242/30	240.44.113.226	FMC_IPSEC_PROFILE_2	SiteN_VTI
Tunnel3	SiteT_New_vti	169.254.130.26/30	244.156.237.220	FMC_IPSEC_PROFILE_2	SiteT_New_VTI

3.3 IP ADDRESS SPACE OVERVIEW, INTERNAL INTERFACES, VLAN INTERFACES

VLAN	INTERFACE	NAME	SUBNET	CONNECTS TO
310	Port-channel1.310	TRANSIT	10.243.31.240/29	internal firewall Fortinet-transit 10.243.31.246
311	Port-channel1.311	TEMPTRANSIT	10.243.31.248/29	Fortinet 600 (temporary point to point)
320	Port-channel1.320	DMZ_IDP	10.230.134.0/24	IDP proxy DMZ
	Ethernet1/2	DMZ_EXTFW	10.243.31.176/28	EXT firewall PARTNER-EXT-FW_Address 10.243.31.186
	Ethernet1/3	Google_IC	169.254.127.192/29	Google Partner Interconnect, BGP peers 169.254.127.193 and 169.254.12.86 (via Tunnel1)
	Management1/1	management	10.147.50.0/24	management network (FMC 10.147.50.139)

Internal address space reached through the internal firewall (from the static routes): 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 100.91.136.0/24 (Fortinet_Loopbacks), and the five networks advertised to Google (10.243.31.0/25, 10.180.162.0/24, 10.114.102.0/24, 10.229.126.0/24, 10.154.21.0/24).

4 Access Control and NAT

4.1 OBJECTS AND GROUPS NAMING CONVENTION

The FMC holds 1,235 network objects (572 host, 412 network, 197 fqdn, 44 group, 10 range) and 456 port objects. The names of network and port objects follow these families:

FAMILY	MEANING	OBJECTS	EXAMPLES
h_	single host, named by its address in the FMC, numbered for this version	65	h_01, h_02, h_03
n_, nw_	network, named by its address in the FMC, numbered for this version	9	nw_01, nw_02, n_01
Network_Net_	objects imported from the previous Fortinet policy	119	Network_Net_25, Network_Net_26, Network_Net_66
static_	objects used by static routes and NAT	99	static_other_extfw_2, static_other_extfw_1, static_remote_Operation
_	Y corp server, named by role for this version	91	directory_21, jump_31, file_74
-FTD_MIG	migrated by the Firewall Migration Tool	8	Canon_counter-FTD_MIG, PartnerA_SOAP-FTD_MIG, AOL-FTD_MIG
VLAN_address, SiteM_VLAN	internal VLAN subnets	54	VLAN_Romeo_address, VLAN_Oscar_address, VLAN_Sierra_address
Site-	site networks behind VPN	19	SiteP-B-entry, SiteT_Meraki_IF, SiteT_Meraki_Papa_IF
PARTNER<...>	Partner A / Partner B networks	68	PARTNER_ERP-print-SRC5, PARTNER_ERP-print-SRC1, PARTNER_ERP-print-SRC2
GCP / GCVE / GCE	Google Cloud networks	3	GCP_01, GCP_02, GCVE-MGMT
, fqdn_	FQDN objects, named by the domain	197	loadproof.us, smtp.office365.com, anydesk.com
TCP_, UDP_	port objects, named by protocol and port	42	TCP_84431, TCP_custom-01_1, TCP_custom-02_1
	members of a port group, named after the group	182	DNS_tcp_53, DNS_udp_53, DCE-RPC_tcp_135

Appendix A lists every object the configuration uses, grouped by the function that uses it.

Descriptions `routeobject` (48) and `interfaceobject` (57) mark objects created by the migration from the previous Fortinet configuration. On the device, the FMC also generates its own objects: `FMC_INLINE_*` (rule literals), `SVC_<n>` (services), `FMC_VPN_NAT_*` and `CSM_*` (VPN and IPsec).

4.2 SECURITY ZONES

ZONE	TYPE	MODE	INTERFACES	PHYSICAL
SiteT_New_VTI	Security zone	routed	SiteT_New_vti	Tunnel3
SiteN_VTI	Security zone	routed	SiteN_vti	Tunnel2
DMZ_IDP	Security zone	routed	DMZ_IDP	Port-channel1.320
DMZ_EXTFW	Security zone	routed	DMZ_EXTFW	Ethernet1/2
GIC	Security zone	routed	Google_IC, Google_IC_local	Ethernet1/3, Tunnel1
INSIDE-ZONE	Security zone	routed	TRANSIT, TEMPTRANSIT	Port-channel1.310, Port-channel1.311
OUTSIDE-ZONE	Security zone	routed	outside	Ethernet1/1
Transit_IG	Interface group	routed	TRANSIT	Port-channel1.310

core9500 (Port-channel1 parent) and management are in no zone.

4.3 ACCESS CONTROL POLICIES

SETTING	VALUE
Policy	FTD3105-Access-Policy, assigned to FTD-HQ-HA
Rules	157 (144 Allow, 12 Trust, 1 Block); 2 disabled; compiled to 1167 device ACEs (plus 5 prefilter ACEs and 1 default-action ACE)
Default action	Block all traffic, log at connection start to the FMC
Prefilter policy	Default Prefilter Policy (no rules; tunnels allowed and analysed)
Security Intelligence	Block: Global Block List, TID IPv4/IPv6 Block (network); Global Block List for URL, TID URL Block (URL); TID SHA-256 Block (file). Monitor: TID IPv4/IPv6, URL and SHA-256 Monitor. Do-not-block: Global Do-Not-Block Lists. No Talos feed categories selected.
DNS policy	Default DNS Policy (Global Block List for DNS: NXDOMAIN; TID Domain Name Block / Monitor)
SSL/TLS decryption policy	none
Identity policy	none
Intrusion policies used by rules	IPS_Policy_FTD3105_Protect_Balanced (base Balanced Security and Connectivity, prevention); IPS_Policy_FTD3105_Protect_SOC (base Security Over Connectivity, prevention); IPS_Policy_FTD3105_Detect (base Balanced Security and Connectivity, detection only)
Intrusion policy defaults	no rule overrides, suppressions or thresholds in any of the three
Default intrusion policy / variable set	No Rules Active / Default-Set (all network variables any)
Network analysis policy	Balanced Security and Connectivity, inline, no custom rules
Network discovery	applications only, all networks (0.0.0.0/0, ::/0)
Threat Intelligence Director	enabled
Logging	37 rules also send connection events to syslog; IPS and file events use the platform syslog settings
Time range	Schedule-IDP-LIC: Thursday 13:00 to 15:00 (time zone object Local)

Device level settings compiled on the FTD, outside the access policy:

SETTING	VALUE
Inspections (global_policy, default class)	dns (preset_dns_map, max message 512), ftp, h323 h225, h323 ras, rsh, rtsp, sqlnet, skinny, sunrpc, sip, netbios, tftp, icmp, icmp error, ip-options
Inspections (class_snmp)	snmp on UDP/custom-03
TCP normalisation	class-default: UM_STATIC_TCP_MAP
Flow offload	enabled
Threat detection	basic threat on; access-list statistics on; TCP intercept statistics off
Timeouts	xlate 3:00:00, pat-xlate 0:00:30, conn 1:00:00, half-closed 0:10:00, udp 0:02:00, icmp 0:00:02, sip 0:30:00, uauth 0:05:00 absolute, conn-holddown 0:00:15, igp stale-route 0:01:10
Snort	preserve-connection on; multichannel load balancing on

4.3.1 Rule Base Structure and Ordering

Rules are evaluated top down, first match. Y corp orders them in FMC categories by function; the categories and their rules are listed below in policy order. Within each category the rules are grouped by direction, from source zone to destination zone. In the tables, IPS shows the intrusion policy without its `IPS_Policy_FTD3105_` prefix; Log shows B (connection start), E (connection end) and S (also to syslog); every logging rule sends to the FMC.

#	CATEGORY	RULES	ALLOW	TRUST	BLOCK	RULE NUMBERS
1	Inside-Rules	5	5	0	0	1 to 5
2	INTERNET-IN-Rules	5	5	0	0	6 to 10
3	S2SVPN-INTEGRATOR	2	2	0	0	11 to 12
4	S2SVPN-GCP	3	3	0	0	13 to 15
5	S2SVPN-SiteT	18	18	0	0	16 to 33
6	S2SVPN-LIC	5	5	0	0	34 to 38
7	S2SVPN-PartnerF	3	3	0	0	39 to 41
8	S2SVPN-PARTNERA	9	0	9	0	42 to 50
9	S2SVPN-PARTNERB	24	24	0	0	51 to 74
10	S2SVPN-Google	2	2	0	0	75 to 76
11	S2SVPN-SiteN	4	4	0	0	77 to 80
12	S2SVPN-PartnerH	2	2	0	0	81 to 82
13	SiteM-GCVE	2	2	0	0	83 to 84
14	DMZ_rules	10	10	0	0	85 to 94
15	Internet-out	60	59	1	0	95 to 154
16	Temporary rules	2	0	2	0	155 to 156
17	Default section	1	0	0	1	157 to 157

Inside-Rules (5 rules)

INSIDE-ZONE → INSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
1	VPN_access_ALLOW_Internal	Allow	VPN_access_ALL	any	any	Protect_SOC	ES
2	VPN_access_ALLOW_Internal-Clone-153	Allow	any	VPN_access_ALL	any	Protect_SOC	ES
5	GuestWiFi_to_hrapp.example.com	Allow	Internal-GUEST	Web-Server-HTTP	HTTPS (TCP/443), HTTP (TCP/80)		E

INSIDE-ZONE → OUTSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
3	VPN_access_ALLOW_Internet	Allow	VPN_access_ALL	any	apps: HTTPS, ICMP, HTTP	Protect_SOC	ES
4	Fortinet_Validate_Traffic_2_CDNs	Allow	Fortinet_Loopback4	any	any	Protect_Balanced	E

INTERNET-IN-Rules (5 rules)

OUTSIDE-ZONE → INSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
6	VPN_access	Allow	any	Fortinet_Loopback1, Fortinet_Loopback2, Fortinet_Loopback3, Fortinet_Loopback7, Fortinet_Loopback8, Fortinet_Loopback9	VPN_access_ipsec (UDP/custom-04), HTTPS (TCP/443), VPN_access_ipsec_HQIT (UDP/custom-05)		BE
8	Proxy HTTPS in	Allow	any	Web-Server-HTTP	HTTPS (TCP/443); apps: HTTPS	Protect_SOC	ES
9	SAP SFTP in	Allow	SAP_host_01, SAP_host_02, SAP_host_03, SAP_host_04, hrgw.partner-g.example	Web-Server-HTTP	SSH (TCP/22)	Protect_Balanced	ES
10	PARTNERA SFTP in	Allow	host_03, Partner_A_NonProd_IP, host_04	sftp_43	SSH (TCP/22)	Protect_Balanced	ES

OUTSIDE-ZONE → DMZ_IDP

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
7	DSNAT IDP HTTPS	Allow	any	IDP_VIP	HTTPS (TCP/443)		E

S2SVPN-INTEGRATOR (2 rules)

OUTSIDE-ZONE → INSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
11	INTEGRATOR_MGMT_Accesses	Allow	INTEGRATOR_Office_NET	FAZ, core_sw, host_05, FMCv, FTD3105_1, FTD3105_2	SSH (TCP/22), HTTPS (TCP/443)		E
12	INTEGRATOR_RDP_to_jump_33-32	Allow	INTEGRATOR_Office_NET	jump_33, jump_32	RDP (TCP/3389), RDP_UDP (UDP/3389), ALL_ICMP		E

S2SVPN-GCP (3 rules)

OUTSIDE-ZONE → INSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
13	HQ-GCP_to_sftp_42	Allow	h_04	app_51	RDP (TCP/3389), ALL_ICMP	Detect	E

INSIDE-ZONE → OUTSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
14	sftp_42_to_HQ-GCP	Allow	sftp_42, app_54, app_51	h_05	TCP_custom-06 (TCP/custom-06)	Detect	E
15	HQ_GCP_TEST	Allow	Fortinet_Loopbacks, SiteM_VLAN_Juliet, SiteM_VLAN_Kilo	h_05, h_04	ALL_ICMP		BE

S2SVPN-SiteT (18 rules)

INSIDE-ZONE → SiteT_New_VTI

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
16	NetMgmt_2_SiteT_Staging	Allow	host_network_management	VLAN_Delta_address, S_01	ALL_ICMP	Detect	E
17	NETMGMT_2_SiteT_FORTINET	Allow	host_network_management	SiteT-FG-MGMNT-01, SiteT-FG-MGMNT-02	SNMP_tcp_161-162 (TCP/161-162), SNMP_udp_161-162 (UDP/161-162)		none
19	Support_to_SiteTStaging	Allow	jump_31, deploy_71, jump_32, VPN_access_clients_admin	SiteT_S2SRemote	PING, RDP (TCP/3389), DamewareMRC (TCP/6129), SSH (TCP/22)	Detect	E
20	JUMP-Server_to_SiteT-NW-MGMT	Allow	jump_31, jump_32, VPN_access_clients_admin	SiteT-NW-MGMT	HTTPS (TCP/443), SSH (TCP/22)	Detect	E
21	JUMP-Server_to_SiteT-PRN	Allow	jump_31	SiteT-PRN	HTTPS (TCP/443), HTTP (TCP/80), Printer-webmgmt (TCP/8000), Canon-remote-operation-ports	Detect	E

SiteT_New_VTI → INSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
18	SiteT_FORTINET_2_NETMGMT	Allow	SiteT-FG-MGMNT-01, SiteT-FG-MGMNT-02	host_network_management	SNMP_tcp_161-162 (TCP/161-162), SNMP_udp_161-162 (UDP/161-162)		none
31	SiteT-OF_to_app_56	Allow	SiteT-OF	app_56	HTTPS (TCP/443)	Protect_Balanced	E
32	SiteT-PRN_to_mail_relay_72	Allow	SiteT-PRN	mail_relay_72	SMTP (TCP/25)	Protect_Balanced	E

INSIDE-ZONE → OUTSIDE-ZONE, SiteT_New_VTI

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
22	deploy_71_to_SiteT-Staging-Office	Allow	deploy_71	SiteT-OF, net_01	DCE-RPC, PDQ	Detect	E
23	SiteM_VLAN_Lima_to_SiteT-Staging	Allow	host_06	VLAN_Delta_address	SMB (TCP/445), ALL_ICMP	Protect_Balanced	E

OUTSIDE-ZONE, INSIDE-ZONE → SiteT_New_VTI

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
24	PARTNER-Remote_to_SiteT-Staging	Allow	h_06	VLAN_Delta_address	RDP (TCP/3389)	Detect	E

SiteT_New_VTI, OUTSIDE-ZONE → INSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
25	VLAN_Papa - Meraki In1_#527	Allow	SiteT-OF, VLAN_Delta_address	directory_21, directory_22	Windows_AD	Protect_Balanced	E

OUTSIDE-ZONE, SiteT_New_VTI → INSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
26	SiteT-VLANs_to_DCs	Allow	SiteT_S2SRemote	directory_21, directory_22	Windows_AD	Protect_Balanced	E
27	SiteT-Staging-OF_to_pki_73	Allow	VLAN_Delta_address, SiteT-OF	pki_73	DCE-RPC, HTTP (TCP/80)	Protect_Balanced	E
28	SiteT-Staging_to_file_74	Allow	VLAN_Delta_address	file_74	SMB (TCP/445)	Protect_Balanced	E
30	SiteT-OF-VLAN_Delta_to_SCCM	Allow	VLAN_Delta_address, SiteT-OF	update_75	WSUS_PORTS (TCP/8530-8531), WSUS_PORTS_2, ALL_ICMP	Protect_Balanced	E

OUTSIDE-ZONE, SiteT_New_VTI → OUTSIDE-ZONE, INSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
29	SiteT-Staging_to_LIC	Allow	VLAN_Delta_address	LIC_01	LIC (TCP/1688)	Protect_Balanced	E

SiteT_New_VTI → OUTSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
33	SiteT-OF_to_NET	Allow	SiteT-OF	any	ALL_ICMP, HTTPS (TCP/443), HTTP (TCP/80)	Protect_Balanced	E

S2SVPN-LIC (5 rules)

INSIDE-ZONE → OUTSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
34	HQ_LIC_LIC_access	Allow	any	LIC_DESTINATIONS	LIC (TCP/1688), ALL_ICMP	Detect	BE
37	HQ_LIC_ITSM_access	Allow	VPN_access_clients, YC-OF1, YC-OF2	LIC_02, LIC_03, LIC_04	HTTPS (TCP/443)	Detect	BE

SiteT_New_VTI → OUTSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
35	SiteT-OF-Staging_to_HQ_LIC	Allow	SiteT-LIC	LIC_DESTINATIONS	LIC (TCP/1688), ALL_ICMP	Detect	BE

DMZ_IDP → OUTSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
36	HQ_LIC_LIC_access_DMZ_IDP	Allow	IDP_WAP01, IDP_WAP02	LIC_DESTINATIONS	LIC (TCP/1688), ALL_ICMP; time: Schedule-IDP-LIC	Detect	BE

OUTSIDE-ZONE → INSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
38	HQ-SAP_to_Print-SiteR	Allow	Print_Server, Print-Subnets	VLAN_Charlie_address	Printing	Detect	E

S2SVPN-PartnerF (3 rules)

OUTSIDE-ZONE → INSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
39	PartnerF_to_hr_web_86	Allow	PartnerF_remote_subnet_1	host_07	HTTP (TCP/80), ALL_ICMP, HTTPS (TCP/443), TCP_custom-07 (TCP/custom-07), TCP_custom-08 (TCP/custom-08)	Protect_Balanced	E

INSIDE-ZONE → OUTSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
40	hr_web_86_to_PartnerF	Allow	host_07	PartnerF_remote_subnet_1	HTTP (TCP/80), ALL_ICMP, HTTPS (TCP/443), TCP_custom-07 (TCP/custom-07), TCP_custom-08 (TCP/custom-08)	Protect_Balanced	E
41	Clients_to_PartnerF-RDP	Allow	YC-OF1, YC-OF2, VPN_access_clients	PartnerF-RDP	PartnerF-rdp-service (TCP/custom-09), ALL_ICMP		E

S2SVPN-PARTNERA (9 rules)

OUTSIDE-ZONE → OUTSIDE-ZONE, INSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
42	V-PartnerA-Carbonite_to_app_55	Trust	h_07, h_08	app_55	Carbonite_Double_Take		ES

OUTSIDE-ZONE, INSIDE-ZONE → OUTSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
43	app_55_to_V-PartnerA-Carbonite	Trust	app_55	host_08, host_09	Carbonite_Double_Take		ES

OUTSIDE-ZONE → INSIDE-ZONE, OUTSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
44	PARTNER-Remote_to_SiteT-Staging_RDP	Trust	h_06	VLAN_Delta_address	RDP (TCP/3389)		ES
45	PARTNER-ZPA_to_app_52	Trust	PARTNER-A-HOSTS	app_52	RDP (TCP/3389)		ES

OUTSIDE-ZONE → INSIDE-ZONE, DMZ_EXTFW

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
46	EXT_IPSEC_enc_IN	Trust	EXT_IPSEC_PEERS	PARTNER-EXT-FW_Address	any		E

INSIDE-ZONE, DMZ_EXTFW → OUTSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
47	EXT_IPSEC_enc_OUT	Trust	PARTNER-EXT-FW_Address	EXT_IPSEC_PEERS	any		ES
48	PARTNER-EXT-FW_to_PARTNER-A-FW-MGMT	Trust	PARTNER-EXT-FW_Address	PARTNER_A_FW_MGMT_SRC1, PARTNER_A_FW_MGMT_SRC2, PARTNER_A_FW_MGMT_SRC3, PARTNER_A_FW_MGMT_SRC4	8888, NTP, PING, TCP_49 (TCP/49), SNMP_UDP (UDP/161-162), TCP_541 (TCP/541), TCP_514 (TCP/514), UDP_514 (UDP/514), HTTP (TCP/80), HTTPS (TCP/443), TCP_8890 (TCP/8890), DNS		ES
50	VLAN-Mike_to_PARTNER-A-FW-MGMT	Trust	SiteM_VLAN_Mike	PARTNER_A_FW_MGMT_SRC1, PARTNER_A_FW_MGMT_SRC2, PARTNER_A_FW_MGMT_SRC3, PARTNER_A_FW_MGMT_SRC4, PARTNER_A_FW_MGMT_SRC5	8888, 8889, PING, TCP_49 (TCP/49), UDP_123 (UDP/123), SNMP_UDP (UDP/161-162), TCP_541 (TCP/541), TCP_514 (TCP/514), UDP_514 (UDP/514), HTTP (TCP/80), HTTPS (TCP/443), TCP_8890 (TCP/8890), TCP_custom-10 (TCP/custom-10), TCP_custom-11 (TCP/custom-11), SSH (TCP/22), UDP_custom-12 (UDP/custom-12), DNS		ES

OUTSIDE-ZONE → DMZ_EXTFW, INSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
49	PARTNER-A-FW-MGMT_to_VLAN-Mike	Trust	PARTNER_A_FW_MGMT_SRC1, PARTNER_A_FW_MGMT_SRC2, PARTNER_A_FW_MGMT_SRC3, PARTNER_A_FW_MGMT_SRC4, PARTNER_A_FW_MGMT_SRC5	SiteM_VLAN_Mike	8888, 8889, PING, TCP_49 (TCP/49), UDP_123 (UDP/123), SNMP_UDP (UDP/161-162), TCP_541 (TCP/541), TCP_514 (TCP/514), UDP_514 (UDP/514), HTTP (TCP/80), HTTPS (TCP/443), TCP_8890 (TCP/8890), TCP_custom-10 (TCP/custom-10), TCP_custom-11 (TCP/custom-11), SSH (TCP/22), DNS		E

S2SVPN-PARTNERB (24 rules)

INSIDE-ZONE → OUTSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
51	erp_61_to_SOAPPartnerB	Allow	erp_61	svc-cert-ha.partner-b.example	HTTPS (TCP/443)	Detect	E
52	VLAN-Alpha-Bravo_to_V-PartnerB-ERP	Allow	SiteM_VLAN_Alpha, SiteM_VLAN_Bravo	erpprod.partner-b.example, Telnet_ERP_PartnerB_Prod	TCP_custom-13 (TCP/custom-13), ALL_ICMP		E
54	VLAN-Alpha_to_V_PARTNER_ERP	Allow	SiteM_VLAN_Alpha	erpprod.partner-b.example	custom-01 (TCP/custom-01)		E
56	app_54_to_V_PartnerB_Carbonite	Allow	app_54	host_10, h_09, h_10	Carbonite_Double_Take		E
60	VLAN-Echo_to_svc-partner	Allow	SiteM_VLAN_Echo	host_11, svc-ext-ha.partner-b.example	ALL_ICMP, HTTPS (TCP/443)		E
62	VLAN-Alpha_to_V_PartnerB-ERP	Allow	SiteM_VLAN_Alpha	rpc01.partner-b.example, rpc02.partner-b.example	TCP_8080 (TCP/8080)	Detect	E

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
63	VLAN-Alpha_to_V_PartnerB_ERP-HTTPS	Allow	SiteM_VLAN_Alpha	rpc01.partner-b.example, rpc02.partner-b.example, erpprod.partner-b.example, erpalt.partner-b.example	TCP_84431 (TCP/8443), HTTPS (TCP/443)	Detect	E
68	VLAN-Alpha_to_V_PartnerB_ERP-ALT	Allow	SiteM_VLAN_Alpha	erpalt.partner-b.example	custom-02 (TCP/custom-02)		E
69	VLAN-Alpha_to_V_PartnerB_ERP-Duplicated61	Allow	SiteM_VLAN_Alpha	rpc02.partner-b.example, rpc01.partner-b.example	8080 (TCP/8080)	Detect	E
71	VLAN-Alpha-Bravo_to_V_PARTNER_ERP_PROD	Allow	SiteM_VLAN_Alpha, SiteM_VLAN_Bravo	Telnet_ERP_PartnerB_Prod	custom-13 (TCP/custom-13), ALL_ICMP	Detect	E
72	VLAN-Alpha-Bravo_to_V_PARTNER_ERP_TEST	Allow	SiteM_VLAN_Alpha, SiteM_VLAN_Bravo	Telnet_ERP_PartnerB_Test	custom-14 (TCP/custom-14)	Detect	E
74	VLAN-Alpha_to_V_PartnerB_ERP-TCPcustom-01_1	Allow	SiteM_VLAN_Alpha	rpc01.partner-b.example, rpc02.partner-b.example, erpprod.partner-b.example, erpalt.partner-b.example	TCP_8080 (TCP/8080), TCP_custom-01_1 (TCP/custom-01), TCP_custom-15 (TCP/custom-15)	Detect	E

OUTSIDE-ZONE → INSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
53	V_PartnerB_to_app_51	Allow	PARTNER_remote	app_51	ALL_ICMP, RDP (TCP/3389)		E
55	V_PartnerB_Carbonite_to_app_54	Allow	host_10, h_09	app_54	Carbonite_Double_Take		E
57	V_PartnerB_to_sftp_42	Allow	host_13	sftp_42	SSH (TCP/22)		E
58	PARTNER-VPN_to_fwmgmt_76-app_51-VLAN-Hotel	Allow	PARTNER_remote	app_51, SiteM_VLAN_Hotel, fwmgmt_76	any		E
59	vpn_PARTNER-VPN_r~#445_UNSUPPORTED	Allow	PARTNER_B_Remote	SiteM_VLAN_Alpha, SiteM_VLAN_Bravo, SiteM_VLAN_Charlie, SiteM_VLAN_Juliet, SiteM_VLAN_Echo, SiteM_VLAN_Foxtrot, SiteM_VLAN_Kilo, SiteM_Servers	any	Protect_Balanced	E
64	V_PartnerB_ERP_to_VLAN-Alpha	Allow	rpc01.partner-b.example, rpc02.partner-b.example, erpprod.partner-b.example, erpalt.partner-b.example	SiteM_VLAN_Alpha	TCP_9100 (TCP/9100)	Detect	E
65	V_PartnerB_ERP-PROD_to_VLAN-Alpha	Allow	erpprod.partner-b.example	SiteM_VLAN_Alpha	TCP_custom-01_2 (TCP/custom-01)	Detect	E
66	V_PartnerB_ERP-ALT_to_VLAN-Alpha	Allow	erpalt.partner-b.example	SiteM_VLAN_Alpha	TCP_custom-02_2 (TCP/custom-02)	Detect	E

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
67	V_PartnerB_ERP_to_VLAN-Alpha-Bravo-PING	Allow	erpprod.partner-b.example, Telnet_ERP_PartnerB_Prod	SiteM_VLAN_Alpha, SiteM_VLAN_Bravo	ALL_ICMP	Detect	E
70	V_PartnerB_ERP_to_VLAN-Charlie	Allow	rpc02.partner-b.example, erpprod.partner-b.example, erpalt.partner-b.example	rpc01.partner-b.example, SiteM_VLAN_Charlie	TCP9100 (TCP/9100)	Detect	E

INSIDE-ZONE, DMZ_EXTFW → OUTSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
61	PARTNER-EXT-FW_to_PARTNER	Allow	PARTNER-EXT-FW_Address, PARTNER-EXT-FW_Loopback	PARTNER_NET_01	IKE, 8888, 8889, PING, TCP_49 (TCP/49), UDP_123 (UDP/123), SNMP_UDP (UDP/161-162), TCP_541 (TCP/541), TCP_514 (TCP/514), UDP_514 (UDP/514), HTTP (TCP/80), HTTPS (TCP/443), TCP_8890 (TCP/8890), TCP_custom-10 (TCP/custom-10), TCP_custom-11 (TCP/custom-11), ESP_		E

OUTSIDE-ZONE → INSIDE-ZONE, DMZ_EXTFW

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
73	PARTNER_to_PARTNER-EXT-FW	Allow	PARTNER_NET_01	PARTNER-EXT-FW_Address, PARTNER-EXT-FW_Loopback	IKE, 8888, PING, SSH (TCP/22), TCP_541 (TCP/541), TCP_custom-11 (TCP/custom-11), UDP9443 (UDP/9443), TCP_514 (TCP/514), HTTP (TCP/80), HTTPS (TCP/443), TCP_8890 (TCP/8890), UDP_514 (UDP/514), SNMP_UDP (UDP/161-162), ESP_		E

S2SVPN-Google (2 rules)

GIC → INSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
75	Google_IC_in	Allow	GCP_01, GCP_02, Google_35.199.192.0__19	SiteM_ESXI-MGMT, jump_31, directory_21, directory_22, HCX-Local, HCX-MGMT, static_remote_Test_vMotion, backup_77	any		B

INSIDE-ZONE → GIC

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
76	Google_IC_out	Allow	SiteM_ESXI-MGMT, jump_31, directory_21, directory_22, HCX-Local, HCX-MGMT, static_remote_Test_vMotion, backup_77	GCP_01, GCP_02	any		BE

S2SVPN-SiteN (4 rules)

SiteN_VTI → INSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
77	SiteN_APs_to_WLC	Allow	SiteN-NW-MGMT	host_05	ALL_ICMP, CAPWAP (UDP/5246-5247), NTP		E
80	SiteN_FORTINET_2_NETMGMT	Allow	SiteN-FG-MGMNT-01, SiteN-FG-MGMNT-02	host_network_management	SNMP_tcp_161-162 (TCP/161-162), SNMP_udp_161-162 (UDP/161-162)		none

INSIDE-ZONE → SiteN_VTI

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
78	Jump-servers_to_SiteN-NW-MGMT	Allow	Tango, VPN_access_clients_admin	SiteN-NW-MGMT	ALL_ICMP, HTTPS (TCP/443), SSH (TCP/22)		E
79	NETMGMT_2_SiteN_FORTINET	Allow	host_network_management	SiteN-FG-MGMNT-01, SiteN-FG-MGMNT-02	SNMP_tcp_161-162 (TCP/161-162), SNMP_udp_161-162 (UDP/161-162)		none

S2SVPN-PartnerH (2 rules)

OUTSIDE-ZONE → INSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
81	PartnerHJumpServer_to_jump_34	Allow	PartnerH-JumpServer	jump_32, jump_34	RDP (TCP/3389), RDP_UDP (UDP/3389), ALL_ICMP		none

INSIDE-ZONE → OUTSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
82	jump_34_to_PartnerHJumpServer	Allow	jump_32, jump_34	PartnerH-JumpServer	ALL_ICMP		none

SiteM-GCVE (2 rules)

INSIDE-ZONE → GIC

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
83	from_SiteM_to_GCVE	Allow	host_sftp_44, SiteM_ESXI-MGMT, SiteM_vMotion, SiteM_ESXI-GCE-Uplink, directory_21, directory_22	GCP_02, GCVE-MGMT	any	Protect_Balanced	ES

GIC → INSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
84	from_GCVE_to_SiteM	Allow	GCP_02, GCVE-MGMT, Google_35.199.192.0__19	host_sftp_44, SiteM_ESXI-MGMT, SiteM_vMotion, SiteM_ESXI-GCE-Uplink	any	Protect_Balanced	ES

DMZ_rules (10 rules)

DMZ_IDP → INSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
85	IDP-DMZ-Proxy_to_IDP01-02	Allow	DMZ_IDP_Proxy_Hosts	idp_81, idp_82, NLB-IDP	HTTPS-only443 (TCP/443), ALL_ICMP	Detect	E

DMZ_IDP → OUTSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
86	IDP_to_NET	Allow	IDP_VIP	any	HTTP (TCP/80), HTTPS (TCP/443), ALL_ICMP		none
87	IDP-DMZ_to_NET	Allow	DMZ_IDP_Proxy	any	ALL_ICMP, HTTP (TCP/80), HTTPS (TCP/443)	Detect	E
88	IDP-DMZ_to_WAN-DNS	Allow	DMZ_IDP_Proxy	one.one.one.one	apps: DNS	Detect	E

INSIDE-ZONE, DMZ_IDP → OUTSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
89	IDP-DMZ_to_NET-NTP	Allow	IDP_WAP01, IDP_WAP02, dmz_proxy_83, dmz_proxy_84, IDP_WAP	pool.ntp.org	NTP	Detect	E

INSIDE-ZONE → INSIDE-ZONE, DMZ_IDP

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
90	jump_31-to-IDP-DMZ	Allow	jump_31	DMZ_IDP_Proxy	SSH (TCP/22), ALL_ICMP, RCP (TCP/135)	Detect	E

INSIDE-ZONE → DMZ_IDP

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
91	idp_81-82_to_WAP01-02	Allow	idp_81, idp_82	IDP_WAP01, IDP_WAP02	RDP (TCP/3389), HTTPS (TCP/443)	Detect	E
92	NetMgmt_to_IDP-DMZ	Allow	host_network_management	IDP_WAP01, IDP_WAP02, IDP_VIP, dmz_proxy_83, dmz_proxy_84	NetMgmt (TCP/10050-10051)	Detect	E
93	jump_31-to-WAP01-02-VIP	Allow	jump_31	IDP_WAP01, IDP_WAP02, IDP_VIP	RDP (TCP/3389), ALL_ICMP	Detect	E
94	VPN_access_to_IDP-DMZ	Allow	VPN_access_clients, VPN_access_clients_admin	IDP_WAP01, IDP_WAP02, IDP_VIP	apps: HTTPS, ICMP	Detect	E

Internet-out (60 rules)

INSIDE-ZONE → OUTSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
95	MSTeams_to_Internet_Stun	Allow	Fortinet-transit	any	apps: MSTeams-App	Protect_Balanced	E
96	Fortinet Internet Access	Allow	Fortinet-transit	any	icmp_req, HTTPS (TCP/443), HTTP (TCP/80), DNS_over_UDP (UDP/53), DNS_over_TCP (TCP/53), TCP_custom-16 (TCP/custom-16), TCP_custom-17 (TCP/custom-17), UDP_21116 (UDP/21116)	Protect_Balanced	E
100	Fortinet-Guest_DNS-Proxy	Allow	Fortinet-Guest-DNS-Proxy-LO	ISP-DNS_Server_01, ISP-DNS_Server_02	DNS		none
101	Fortinet Internet Access-SAML	Allow	Fortinet_Loopback1	any	src HTTPS (TCP/443)		E
102	VPN_access_users_to internet	Trust	VPN_access_ALL	sap01.partner-c.example, sap-router-01.partner-c.example	SAP_SAP01_PC_ports_tcp_3299 (TCP/3299), HTTPS (TCP/443), HTTP (TCP/80)		E
103	from_Internal-GUEST_to_NET	Allow	Internal-GUEST	any	DNS, VodaFemtoCell, LINEmessenger, IPSEC-NAT-Traversal, HTTPS (TCP/443)	Detect	B
104	from_Internal-GUEST_to_Viber	Allow	Internal-GUEST	viber.com, amazonaws.com	viber-ports	Protect_Balanced	E
105	PartnerD-FTP	Allow	sftp_41	ftp4.partner-d.example, sftp.partner-e.example	SSH (TCP/22)	Protect_Balanced	ES
106	YC-OF1-OF2-WDS_to_NET	Allow	YC-OF1, YC-OF2, SiteM_WDS_Install	any	ALL_ICMP, HTTP (TCP/80), HTTPS (TCP/443)	Protect_Balanced	ES
107	YC-OF1-OF2_to_SAP	Allow	YC-OF1, YC-OF2	SAP_SAP01_PC1, sap-router-01.partner-c.example	SAP_SAP01_PC_ports		ES
108	Corp-Networks_to_Viber	Allow	YC-OF1, YC-OF2	amazonaws.com, viber.com, Amazon_EDL	viber-ports	Protect_Balanced	ES
109	Xray_to_NET	Allow	SiteM_Xray	tenant.sentinelone.net, portal.partner-a.example, sectigostore.com, crt.sectigo.com	ALL_ICMP, HTTP (TCP/80), HTTPS (TCP/443)	Protect_Balanced	ES
110	Xray_to_SAP	Allow	SiteM_Xray	SAP_SAP01_PC	SAP_sap01_pc		ES
111	Yankee_to_NET	Allow	SiteM_VLAN_Echo, SiteM_VLAN_Golf, SiteM_VLAN_Foxtrot, SiteM_VLAN_Hotel	tenant.sentinelone.net	ALL_ICMP, HTTPS (TCP/443)	Protect_Balanced	ES
112	VLAN-Alpha_to_GoogleDNS	Allow	SiteM_VLAN_Alpha	Google_DNS	DNS		ES
113	VLAN_Alpha_to_MSExchange	Allow	SiteM_VLAN_Alpha	Microsoft_Range_5	IPSEC-NAT-Traversal, HTTP (TCP/80), HTTPS (TCP/443)	Protect_Balanced	E
114	VLAN-Alpha_to_SAP	Allow	SiteM_VLAN_Alpha	sap01.partner-c.example, sap-router-01.partner-c.example	SAP_sap01_pc2	Protect_Balanced	E

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
115	VLAN-Charlie_to_CanonCloud	Allow	SiteM_VLAN_Charlie	Canon_counter-FTD_MIG	HTTPS (TCP/443), TCP_84431 (TCP/8443)	Protect_Balanced	E
116	mail_relay_72_to_MSExchange	Allow	mail_relay_72	smtp.office365.com, Outlook_SMTP_Server, sub_Microsoft-office365_Range_1, sub_Microsoft-office365_Range_2	SMTP-TX (TCP/587), SMTP (TCP/25), HTTPS (TCP/443)	Protect_Balanced	E
117	from_ITSM_TO_Microsoft_OAuth2_HTTPS	Allow	host_itsm_85	fqdn_sts.windows.net, fqdn_login.microsoftonline.com	HTTPS (TCP/443)	Protect_Balanced	E
118	from_ITSM_TO_MicrosoftEXO#587_SMTP	Allow	host_itsm_85	outlook.office365.com, smtp.office365.com, Outlook_SMTP_Server, sub_Microsoft_office365_Range_3, sub_Microsoft-office365_Range_2, sub_Microsoft-office365_Range_1, sub_Microsoft-office365_Range_4	SMTP-TX (TCP/587), SMTP (TCP/25), IMAPS (TCP/993)	Protect_Balanced	E
119	SiteM-Servers_to_Zebra.com	Allow	SiteM_Servers	Zebra.com	HTTPS (TCP/443), HTTP (TCP/80)		ES
120	file_74_to_PartnerD	Allow	file_74	b2b.partner-d.example, sftp.partner-e.example	SSH (TCP/22)		ES
121	Linux-servers_to_Repo	Allow	host_network_management, host_syslog_server	any	HTTPS (TCP/443), HTTP (TCP/80)		E
126	FMC_to_NET	Allow	FMCv	nelreports-cisco	HTTP (TCP/80), HTTPS (TCP/443)		E
127	Firewalls_to_NET	Allow	FG-MGMNT-01, FG-MGMNT-02, FG-MGMNT-03, FG-MGMNT-04, FMCv, FTD3105_1, FTD3105_2	any	ALL_ICMP, DNS, HTTPS (TCP/443), HTTP (TCP/80)		E
128	VLAN-Alpha_to_NET	Allow	SiteM_VLAN_Alpha	any	HTTPS (TCP/443)	Protect_Balanced	ES
129	from_Alpha_to_AKAMAI_HTTP/S	Allow	SiteM_VLAN_Alpha	AKAMAI_EDL	HTTPS (TCP/443), HTTP (TCP/80)	Protect_Balanced	ES
130	erp_61_to_PartnerASoap	Allow	erp_61	PartnerA_SOAP-FTD_MIG	HTTPS (TCP/443)	Protect_Balanced	E
131	app_56_to_Rates	Allow	app_56	RATES_FQDN, date.nager.at, fqdn_dev.azure.com	HTTPS (TCP/443), HTTP (TCP/80)		ES
132	app_59_to_Smartsheet	Allow	app_59	api.smartsheet.eu, api.smartsheet.com	HTTP (TCP/80), HTTPS (TCP/443)		ES
133	VLAN-Hotel_to_PartnerASoap	Allow	SiteM_VLAN_Hotel	PartnerA_SOAP-FTD_MIG	HTTPS (TCP/443)	Protect_Balanced	ES
134	VLAN-Golf_to_PartnerASoap	Allow	SiteM_VLAN_Golf	PartnerA_SOAP-FTD_MIG	HTTPS (TCP/443)	Protect_Balanced	E
135	SiteM_VLAN_Golf_to_Portal-Access-PartnerA	Allow	SiteM_VLAN_Golf	Portal-Access_PARTNERA	HTTPS (TCP/443), Portal-Access-PartnerA_UA (TCP/custom-18), Portal-Access-PartnerA-LB (TCP/8883)	Protect_Balanced	E

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
136	app_57_to_cacerts.digicert.com	Allow	app_57	cacerts.digicert.com	HTTP (TCP/80)		ES
137	erp_61-62-app_58_to_SAP	Allow	erp_61, erp_62, app_58, erp_63	sap01.partner-c.example_SAP, sap-router-01.partner-c.example	SAP_SAP01_PC_ports, SAP_prod_router_pc (TCP/custom-19)		E
138	NetMgmt_to_SAP	Allow	host_network_management	sap01.partner-c.example_SAP, sap-router-01.partner-c.example	SAP_tcp_3299 (TCP/3299)		E
139	app_58_to_SAP	Allow	app_58	SAP_SAP01_PC1	SAP_SAP01_PC_ports		ES
140	PARTNER-Guest_to_NET	Allow	PartnerA-Guest, PartnerB-Guest	any	NTP, ALL_ICMP, HTTP (TCP/80), HTTPS (TCP/443), DNS	Protect_Balanced	ES
141	External_GUEST_to_NET	Allow	External-GUEST	any	ALL_ICMP, HTTP (TCP/80), HTTPS (TCP/443), DNS, IMAPS (TCP/993)	Protect_Balanced	ES
142	EXT_GUEST_to_SiteKVPN	Allow	External-GUEST	SiteKOpenVPN	OPENVPN		E
143	from_VLANS_to_Sectigo	Allow	SiteM_VLAN_November, SiteM_VLAN_Echo, SiteM_VLAN_Golf	crt.sectigo.com, sectigostore.com	HTTPS (TCP/443), HTTP (TCP/80)	Protect_Balanced	ES
144	from_VLAN-November_to_loadproof.us	Allow	SiteM_VLAN_November	loadproof.us	HTTPS (TCP/443)	Protect_Balanced	ES
145	from_VLAN-November_to_MS-Range	Allow	SiteM_VLAN_November	Microsoft_Office_365, Microsoft_Range_5	IPSEC-NAT-Traversal, HTTP (TCP/80), HTTPS (TCP/443)	Protect_Balanced	E
146	from_VLAN-November_to_GooglePlay	Allow	SiteM_VLAN_November	Google_play	IPSEC-NAT-Traversal, HTTP (TCP/80), HTTPS (TCP/443)		E
147	from_VLAN-November_to_voWifi	Allow	SiteM_VLAN_November	h_11, h_12	IKE		E
148	from_VLAN-November_to_GoogleDNS	Allow	SiteM_VLAN_November	Google_DNS	DNS		E
149	Printers_to_Canon URLs	Allow	YC-PRN	Canon_counter-FTD_MIG	HTTPS (TCP/443), TCP_84431 (TCP/8443)		E
150	YC-IoT_to_NET	Allow	YC-IoT	fqdn_prusa3d.com	HTTPS (TCP/443)		E
151	from_NDR_to_NET	Allow	NDR_Sensor	NDR_ext_url, tenant.sentinelone.net	HTTP (TCP/80), ALL_ICMP, HTTPS (TCP/443)	Protect_Balanced	ES
152	Server_Update_Policy	Allow	sub_TS-PartnerH, SiteM_VLAN_Juliet, SiteM_VLAN_India, SiteM_Quebec, SiteM_Servers, sub_TS-INTEGRATOR, SiteM_VLAN_Kilo, SiteM_VLAN_Lima, OT-Servers	any	HTTPS (TCP/443), HTTP (TCP/80)	Protect_SOC	E
153	from_jump_31_to_NET-PingTracert	Allow	jump_31	any	ALL_ICMP	Protect_SOC	E

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
154	ESXI-MGMT_Update_Policy	Allow	SiteM_ESXI-MGMT	any	HTTPS (TCP/443)	Protect_SOC	E

any → any

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
97	DC-DNS-Allow	Allow	directory_21, directory_22, ot_dns_91	ISP-DNS_Server_02, ISP-DNS_Server_01	DNS_over_TCP (TCP/53), DNS_over_UDP (UDP/53); apps: DNS		none
98	from_DCs-OT-Servers_to_time_windows_com_NTP	Allow	directory_21, directory_22, ot_ntp_92	time.windows.com	UDP_123 (UDP/123); apps: NTP		none
99	OT-DNS-NTP_to_Pub-DNS-NTP (disabled)	Allow	ot_dns_91, ot_ntp_92	one.one.one.one, Google_DNS	UDP_123 (UDP/123), DNS; apps: NTP, DNS		none
124	NetMgmt-ICMP-monitoring-to-PartnerC-SAProuter	Allow	host_network_management	Last_hop_to_PC_SAP_router	ALL_ICMP		none
125	NetMgmt-ICMP-monitoring	Allow	host_network_management	any	ALL_ICMP		none

DMZ_IDP → OUTSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
122	DMZLinux_Servers_to_Internet_HTTPS Maintenance (disabled)	Allow	host_dmz_proxy_83, host_dmz_proxy_84	any	HTTPS (TCP/443), HTTP (TCP/80)		E
123	DMZLinux_Servers_to_Google_DNS	Allow	host_dmz_proxy_83, host_dmz_proxy_84	Google_DNS_02, 8.8.8.8	DNS_over_TCP (TCP/53), DNS_over_UDP (UDP/53)		E

Temporary rules (2 rules)

INSIDE-ZONE → OUTSIDE-ZONE, INSIDE-ZONE, DMZ_IDP, DMZ_EXTFW

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
155	Network-ManagemementMigration-Out	Trust	nw_03	any	any		E

OUTSIDE-ZONE, INSIDE-ZONE, DMZ_IDP, DMZ_EXTFW → INSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
156	Network-ManagemementMigration-In	Trust	any	nw_03	any		E

Default section (1 rule)

OUTSIDE-ZONE, INSIDE-ZONE → OUTSIDE-ZONE, INSIDE-ZONE

#	RULE	ACTION	SOURCE	DESTINATION	SERVICE / APPLICATION	IPS	LOG
157	DEAFULT-BLOCK-INBOUND	Block	any	any	any		B

87 rules carry the comment "copied from Fortinet_Migrated_Policy", from the migration of the previous Fortinet rule base.

4.4 NAT POLICIES

NAT policy for FTD-HQ-HA: 29 manual rules before auto NAT, 3 auto NAT rules, 0 after auto NAT. The site to site VPN topologies with automatic NAT exemption add their own identity NAT rules on the device (4.4.2).

4.4.1 NAT Rules Before

NAT exemption (identity NAT) for VPN and partner traffic

#	FROM → TO	TYPE	ORIG. SOURCE	ORIG. DESTINATION	ORIG. SERVICE	TRANSL. SOURCE	TRANSL. DESTINATION	TRANSL. SERVICE	DESCRIPTION
2	INSIDE-ZONE → OUTSIDE-ZONE	Static	PARTNERB_LOCAL_GROUP	PARTNERB_REMOTE_GROUP	any	PARTNERB_LOCAL_GROUP	PARTNERB_REMOTE_GROUP		NAT EXEMPT RULES FOR PARTNERB
3	Transit_IG → OUTSIDE-ZONE	Static	jump_34	PartnerH-JumpServer	any	jump_34	PartnerH-JumpServer		
20	INSIDE-ZONE → OUTSIDE-ZONE	Static	HQ_LIC_LOCAL	HQ_LIC_REMOTE	any	HQ_LIC_LOCAL	HQ_LIC_REMOTE		
26	INSIDE-ZONE → OUTSIDE-ZONE	Static	SiteN_S2SLocal	SiteN_S2SRemote	any	SiteN_S2SLocal	SiteN_S2SRemote		
27	INSIDE-ZONE → OUTSIDE-ZONE	Static	SiteT_S2SLocal	SiteT_S2SRemote	any	SiteT_S2SLocal	SiteT_S2SRemote		

Publication, Internet to internal service (destination NAT)

#	FROM → TO	CLIENT (SOURCE)	PUBLIC ADDRESS	PUBLIC PORT	INTERNAL OBJECT	INTERNAL PORT	DESCRIPTION
4	OUTSIDE-ZONE → INSIDE-ZONE	any	interface (247.222.237.1)	VPN_access_ipsec (UDP/custom-04)	Fortinet_Loopback1 (100.91.136.50)	VPN_access_ipsec (UDP/custom-04)	VPN_access IPSEC
5	OUTSIDE-ZONE → INSIDE-ZONE	any	interface (247.222.237.1)	HTTPS (TCP/443)	Fortinet_Loopback1 (100.91.136.50)	HTTPS (TCP/443)	VPN_access
6	OUTSIDE-ZONE → INSIDE-ZONE	any	interface (247.222.237.1)	VPN_access (TCP/custom-20)	Fortinet_Loopback2 (100.91.136.197)	HTTPS (TCP/443)	VPN_access Admins

#	FROM → TO	CLIENT (SOURCE)	PUBLIC ADDRESS	PUBLIC PORT	INTERNAL OBJECT	INTERNAL PORT	DESCRIPTION
7	OUTSIDE-ZONE → INSIDE-ZONE	any	interface (247.222.237.1)	VPN_access2 (TCP/custom-21)	Fortinet_Loopback3 (100.91.136.221)	HTTPS (TCP/443)	VPN_access 2
8	OUTSIDE-ZONE → INSIDE-ZONE	PARENT-HQ-IT	Public_IP_4 (247.222.237.2)	VPN_access_ipsec (UDP/custom-04)	Fortinet_Loopback9 (100.91.136.236)	VPN_access_ipsec (UDP/custom-04)	
9	OUTSIDE-ZONE → INSIDE-ZONE	any	Public_IP_4 (247.222.237.2)	VPN_access_HQIT (TCP/custom-22)	Fortinet_Loopback9 (100.91.136.236)	HTTPS (TCP/443)	
10	OUTSIDE-ZONE → INSIDE-ZONE	any	Public_IP_4 (247.222.237.2)	VPN_access_ipsec (UDP/custom-04)	Fortinet_Loopback7 (100.91.136.104)	VPN_access_ipsec (UDP/custom-04)	VPN_access Partner ipsec
11	OUTSIDE-ZONE → INSIDE-ZONE	any	Public_IP_4 (247.222.237.2)	HTTPS (TCP/443)	Fortinet_Loopback7 (100.91.136.104)	HTTPS (TCP/443)	VPN_access Partner https
12	OUTSIDE-ZONE → DMZ_IDP	any	IDP-PUBLIC (247.222.237.3)	HTTPS (TCP/443)	IDP_VIP (10.230.134.77)	HTTPS (TCP/443)	IDP publication
13	OUTSIDE-ZONE → INSIDE-ZONE	any	Public_IP_2 (247.222.237.5)	SFTP_alt_port (TCP/custom-23)	sftp_41 (10.243.31.237)	SSH (TCP/22)	ssh_publication
14	OUTSIDE-ZONE → INSIDE-ZONE	any	Public_IP_2 (247.222.237.5)	TCP_custom-24 (TCP/custom-24)	sftp_43 (172.31.221.195)	SSH (TCP/22)	sftp_43_PartnerA
15	OUTSIDE-ZONE → INSIDE-ZONE	any	Public_IP_2 (247.222.237.5)	HTTPS (TCP/443)	Web-Server-HTTP (10.243.31.237)	HTTPS (TCP/443)	Proxy HTTPS
28	OUTSIDE-ZONE → INSIDE-ZONE	any	Public_IP_3 (247.222.237.6)	HTTPS (TCP/443)	Fortinet_Loopback8 (100.91.136.193)	HTTPS (TCP/443)	
29	OUTSIDE-ZONE → INSIDE-ZONE	any	Public_IP_3 (247.222.237.6)	VPN_access_ipsec (UDP/custom-04)	Fortinet_Loopback8 (100.91.136.193)	VPN_access_ipsec (UDP/custom-04)	

Outbound source translation (PAT and static)

#	FROM → TO	TYPE	ORIG. SOURCE	ORIG. DESTINATION	ORIG. SERVICE	TRANSL. SOURCE	TRANSL. DESTINATION	TRANSL. SERVICE	DESCRIPTION
1	INSIDE-ZONE → OUTSIDE-ZONE	Dynamic	any	PARTNER_Public_Services	any	interface	PARTNER_Public_Services		
17	Transit_IG → OUTSIDE-ZONE	Dynamic	any	LIC_DESTINATIONS	any	LIC_outbound_PAT	LIC_DESTINATIONS		LIC outbound PAT
18	DMZ_IDP → OUTSIDE-ZONE	Dynamic	DMZ_IDP_Proxy	LIC_DESTINATIONS	any	LIC_outbound_PAT	LIC_DESTINATIONS		LIC outbound PAT

#	FROM → TO	TYPE	ORIG. SOURCE	ORIG. DESTINATION	ORIG. SERVICE	TRANSL. SOURCE	TRANSL. DESTINATION	TRANSL. SERVICE	DESCRIPTION
19	any → OUTSIDE-ZONE	Dynamic	SiteT-LIC	LIC_DESTINATIONS	any	LIC_outbound_PAT	LIC_DESTINATIONS		LIC outbound PAT
21	INSIDE-ZONE → OUTSIDE-ZONE	Dynamic	Fortinet-transit	Intermediate_Server	any	Kilo_VLAN_keepalive_IP	Intermediate_Server		GCP S2S Keepalive traffic
22	INSIDE-ZONE → OUTSIDE-ZONE	Dynamic	Fortinet_Transit_IF_Alias	Intermediate_Server	any	Juliet_VLAN_keepalive_IP	Intermediate_Server		GCP S2S Keepalive traffic 2
23	INSIDE-ZONE → OUTSIDE-ZONE	Dynamic	Fortinet-transit	SiteT_Meraki_IF	any	Fortinet_Server_IF_IP	SiteT_Meraki_IF		
24	INSIDE-ZONE → OUTSIDE-ZONE	Dynamic	Fortinet-transit	SiteT_Meraki_Papa_IF	any	Fortinet_Server_IF_IP	SiteT_Meraki_Papa_IF		
25	Transit_IG → OUTSIDE-ZONE	Dynamic	any	any	any	interface			DEFAULT PAT

NAT reflection, internal client to a published service by its public address

#	FROM → TO	CLIENT (SOURCE)	PUBLIC ADDRESS	PUBLIC PORT	INTERNAL OBJECT	INTERNAL PORT	DESCRIPTION
16	INSIDE-ZONE → INSIDE-ZONE	Internal-GUEST → interface	Public_IP_2 (247.222.237.5)	HTTPS (TCP/443)	Web-Server-HTTP (10.243.31.237)	HTTPS (TCP/443)	

The 29 rules compile to 54 manual NAT lines on the device (a rule on an interface group or zone expands to one line per interface).

4.4.2 Auto NAT Rules

FROM → TO	TYPE	OBJECT	VALUE	TRANSLATED TO	DESCRIPTION
Transit_IG → OUTSIDE-ZONE	Dynamic	Fortinet-transit	10.243.31.246	interface	DEFAULT PAT
Transit_IG → OUTSIDE-ZONE	Dynamic	Fortinet_Loopback1	100.91.136.50	interface	
DMZ_IDP → OUTSIDE-ZONE	Dynamic	DMZ_IDP_Proxy	10.230.134.0/24	IDP-PUBLIC (247.222.237.3)	

VPN NAT exemptions generated by the FMC: 107 identity NAT lines (description "FMC Auto Generated NAT Exempt"), one per protected network pair of the policy based topologies with NAT exemption enabled. They are placed before the manual rules and do not appear in the FMC NAT policy.

4.4.3 NAT Rules After

No rules are configured in the section after auto NAT.

5 Site to Site VPN

Decrypted VPN traffic is not exempt from the access policy (no `sysopt connection permit-vpn`): the S2SVPN rule categories in 4.3.1 are what permits traffic through the tunnels.

Y corp has 10 site to site VPN topologies in the FMC, all point to point, all IKEv2, all terminating on outside (247.222.237.1) of FTD-HQ-HA. 3 are route based (static VTI), 7 are policy based (crypto map CSM_outside_map). Authentication is by pre-shared key in every topology (keys not reproduced).

5.1 IKEV1

IKEv1 is not used. No topology has IKEv1 selected in the FMC, and the device has no `crypto ikev1 enable` and no IKEv1 policy (aggressive mode is disabled, `crypto ikev1 am-disable`). The default site to site group policy lists both protocols (`vpn-tunnel-protocol ikev1 ikev2`), which is the platform default.

5.1.1 IPsec Proposals

None configured.

5.1.2 Policies

None configured.

5.2 IKEV2

5.2.1 IPsec Proposals

IPSEC PROPOSAL (FMC)	ESP ENCRYPTION	ESP INTEGRITY	USED BY
PartnerF_Phase2	AES-256, AES	SHA-256	PartnerF
AES256-SHA256	AES-256	SHA-256	SiteT_New, SiteN
PartnerH_Phase2	AES-256	SHA-512	PartnerH
Google_Interconnect_phase2	AES-256	SHA-512	Google_IC_S2S
Partner_A_Phase2	AES-256	SHA-256	Partner-A
Partner_B_Phase2	AES-GCM-256	NULL	PARTNER_B
AES-GCM-256-SHA1	AES-GCM-256	SHA-1	INTEGRATOR-support
HQ_GCP_Phase2_1	AES-GCM	NULL	HQ_GCP
HQ_LIC_Phase2	AES-256	SHA-256	HQ_LIC

5.2.2 Policies

IKEV2 POLICY (FMC)	PRIORITY	ENCRYPTION	INTEGRITY	PRF	DH GROUP	LIFETIME (S)	USED BY
PartnerF_Phase1		AES-256	SHA	SHA	14	86400	PartnerF
aes256-sha256-gr21		AES-256	SHA256	SHA256	21	86400	SiteT_New, SiteN
PartnerH_Phase1	2	AES-GCM	NULL	SHA, SHA256	21	28800	PartnerH
Google_Interconnect_phase1		AES-256	SHA512	SHA512	19	36000	Google_IC_S2S
Partner_A_Phase1		AES-256	SHA256	SHA256	14	28800	Partner-A
Partner_B_Phase1		AES-GCM-256	NULL	SHA256	19	28800	PARTNER_B
INTEGRATOR-phase1	10	AES-GCM-256	NULL	SHA512, SHA256, SHA384	21	86400	INTEGRATOR-support
HQ_GCP_Phase1_1		AES-GCM	NULL	SHA256	14	36000	HQ_GCP
HQ_LIC_Phase1_1		AES-GCM, AES-GCM-256	NULL	SHA256	14, 5	28800	HQ_LIC
HQ_LIC_Phase1_2	20000	AES-256	SHA256	SHA, SHA256	14, 5	28800	HQ_LIC

On the device these compile to IKEv2 policies 1, 2, 3, 4, 5, 6, 8, 9, 10, 20000 and IPsec proposals CSM_IP_n.

5.3 ROUTE BASED VPNS

TOPOLOGY	PEER	IKEV2 POLICY	IPSEC PROPOSAL	PFS	IPSEC LIFETIME	NAT-T
SiteT_New	244.156.237.220	aes256-sha256-gr21	AES256-SHA256	group 21	28800 s / 4,608,000 KB	on
SiteN	240.44.113.226	aes256-sha256-gr21	AES256-SHA256	group 21	28800 s / 4,608,000 KB	on
Google_IC_S2S	245.78.19.66	Google_Interconnect_phase1	Google_Interconnect_phase2	group 19	10800 s / 4,608,000 KB	on

TOPOLOGY	VTI	LOCAL TUNNEL IP	PEER TUNNEL IP	ZONE	ROUTING INTO THE TUNNEL
SiteT_New	SiteT_New_vti	169.254.130.26/30	169.254.130.25	SiteT_New_VTI	static route SiteT_S2SRemote
SiteN	SiteN_vti	169.254.253.242/30	169.254.253.241	SiteN_VTI	static route SiteN_S2SRemote
Google_IC_S2S	Google_IC_local	169.254.12.85/30	169.254.12.86	GIC	BGP neighbour 169.254.12.86 (AS 16550)

5.4 POLICY BASED VPNS

TOPOLOGY	PEER	IKEV2 POLICY	IPSEC PROPOSAL	PFS	IPSEC LIFETIME	NAT-T
PartnerF	244.63.218.142	PartnerF_Phase1	PartnerF_Phase2	group 14	86400 s / 4,608,000 KB	on
PartnerH	240.128.182.188	PartnerH_Phase1	PartnerH_Phase2	group 21	28800 s / 4,608,000 KB	off
Partner-A	245.157.58.158	Partner_A_Phase1	Partner_A_Phase2	group 14	3600 s / 4,608,000 KB	on
PARTNER_B	245.88.153.87	Partner_B_Phase1	Partner_B_Phase2	group 19	3600 s / 4,608,000 KB	on
INTEGRATOR-support	245.225.126.243	INTEGRATOR-phase1	AES-GCM-256-SHA1	group 19	28800 s / 4,608,000 KB	off
HQ_GCP	245.137.5.245	HQ_GCP_Phase1_1	HQ_GCP_Phase2_1	group 14	10800 s / 4,608,000 KB	on
HQ_LIC	247.5.48.162	HQ_LIC_Phase1_1, HQ_LIC_Phase1_2	HQ_LIC_Phase2	off	43200 s / 4,608,000 KB	on

Protected networks, from Y corp to the peer:

TOPOLOGY	Y CORP NETWORKS (FTD-HQ-HA)	PEER NETWORKS	NAT EXEMPTION	REVERSE ROUTE INJECTION
PartnerF	VPN_access_clients, PartnerF_local_subnet_1, Victor, Uniform	PartnerF_remote_subnet_1	yes	on
PartnerH	jump_34, jump_32	PartnerH-JumpServer	yes	on
Partner-A	host_06, net_01, PARTNER-EXT-FW_Address, app_52, SiteM_VLAN_Golf, app_53	h_06, host_portalinternaluat.partner-a.example, PARTNER_A_FW_MGMT_SRC4, host_09, PARTNER_A_FW_MGMT_SRC3, host_01, host_08, PARTNER_A_ZPA_2, PARTNER_A_ZPA_1, PARTNER_A_ZPA_4, host_02, PARTNER_A_FW_MGMT_SRC5, host_portalinternal.partner-a.example, PARTNER_A_FW_MGMT_SRC2, PARTNER_A_FW_MGMT_SRC1, PARTNER_A_ZPA_3	yes	on
PARTNER_B	SiteM_VLAN_Alpha, Clean_WiFi, n_02, SiteM_VLAN_Echo, nw_01	net_02, net_03, net_04, net_05, net_06, net_07, n_03	no	on
INTEGRATOR-support	jump_33, nw_03, jump_32	INTEGRATOR_Office_NET	yes	on
HQ_GCP	Network_Net_210, Network_Net_206	net_08	yes	on
HQ_LIC	Print_Host_03, YC-OF2, Print_Host_05, IDP_WAP01, IDP_WAP02, Print_Host_11, Print_Host_07, Print_Host_08, Print_Host_02, Print_Host_04, Print_Host_10, VPN_access_clients, Print_Host_06, Print_Host_09, Network_Net_233, Print_Host_01, YC-OF1	LIC_01, LIC_04, Print-Subnets, LIC_05, LIC_03, nw_04, LIC_02	no	on

Common IPsec settings in all topologies: IKE keepalive on (10 s, 2 retries), NAT keepalive 20 s, DF bit copied, fragmentation before encryption, aggressive mode off; SA PMTU aging infinite. IKEv2 local identity: address on the IPsec profile of SiteT_New and SiteN, auto on the INTEGRATOR-support crypto map entry, the device default elsewhere. PFS "group 14" for PartnerF, Partner-A and HQ_GCP is the FMC value; the device line is set pfs without a group. Default site to site group policy: idle timeout 30 min, no session timeout, no VPN filter. The route based tunnel groups use ikev2 route set interface.

6 FTD Platform Settings, Management, Logging and Monitoring

Platform settings policy **Platform-FTD**, assigned to FTD-HQ-HA.

6.1 NETWORK MANAGEMENT, SNMP

SETTING	VALUE
SNMP server	enabled, UDP/161
System contact	integrator
Location	not set
Management host	host_network_management (10.243.31.4), via the management interface
Host settings	SNMPv3, poll and trap, trap port UDP/162, user sa_netmgmt_ftd
SNMPv3 user	sa_netmgmt_ftd, security level Priv (auth and priv), authentication SHA384, encryption AES-256 (credentials not reproduced)
Traps	authentication, link up, link down, cold start, warm start
Community string	present in the configuration (not reproduced)
FXOS (chassis) SNMP	disabled

6.2 LOGGING, SYSLOG

SETTING	VALUE
Logging	enabled; standby unit logging on; timestamps on, RFC 5424
Facility / device ID	23 (local7) / host name
Format	EMBLEM on
Buffer / flash	buffer 9,999,999 bytes; flash logging off
Server queue	512 messages; traffic allowed when a TCP syslog server is down
VPN logging	on, level warnings (list MANAGER_VPN_EVENT_LIST to the FMC)
Trap filter	event list EVENT-List-1 to the syslog servers (19 message IDs)

SYSLOG SERVER	ADDRESS	PROTOCOL / PORT	INTERFACE
syslog_server	10.243.31.94	UDP/514	management
SIEM-Forwarder	10.69.238.252	TCP/custom-25	management

EVENT-List-1 message IDs: 109005, 602303, 721016, 603104, 603106, 113039, 802001, 713228, 722051, 113019, 717052, 602304, 721018, 722049, 722050, 802002, 716057, 722046, 113035.

Syslog message table: 13 IDs listed at their default level, not suppressed (106015, 106023, 302017, 302018, 302020, 302021, 302013, 302014, 302015, 302016, 313001, 313008, 710003).

6.3 TIME SYNCHRONIZATION

SETTING	VALUE
Source	from the FMC (FTD NTP server 127.0.0.2 through sftunnel), local clock as fallback
Status at backup	time synchronised
FMC time source	NTP 10.243.31.65
NTP authentication	off
System clock	UTC
Time zone object (platform)	Local: a named local time zone with a daylight saving rule (value withheld); used by time range objects

7 FMC System Management

7.1 CONFIGURATION

7.1.1 Audit Log

SETTING	VALUE
Send audit log to syslog	on, to syslog-server.example.com, facility USER, severity INFO, JSON
Send audit log to HTTP server	off
Audit log TLS	off

7.1.2 DNS Cache

SETTING	VALUE
DNS resolution caching	on, timeout 300 s
FMC DNS servers	10.243.31.65, 10.243.31.93, search domain example.com

7.1.3 Email Notification

SETTING	VALUE
Mail relay	10.243.31.83, TCP/25
Encryption	none
Authentication	off
From address	cisco@example.com

7.1.4 HTTPS Certificate

SETTING	VALUE
Subject	CN=FMC93.example.com
Alternative names	FMC93.example.com, FMC93, 10.147.50.139
Issuer	Org-Sub-CA01 (root Org-Root-CA)
Validity	2025-05-19 to 2028-05-18
Client certificates	not required
TLS	1.2 and 1.3

7.1.5 Management Interface

SETTING	VALUE
eth0	10.147.50.139/24, gateway 10.147.50.65, MTU 1500, IPv6 off
Services	management traffic and event traffic
Host name	fmc93.example.com
Remote management port	8305
Proxy	off
Access list	HTTPS TCP/443 from any; SSH TCP/22 from any
SSH	root login off, 3 attempts, 1 session; SHA-2 MACs; AES-GCM, ChaCha20, AES-CTR

7.1.6 SNMP

SETTING	VALUE
Agent	UDP/161 (IPv4 and IPv6)
User	sa_netmgmt_ftd, SNMPv3 read only, auth and priv (credentials not reproduced)

7.1.7 Time Synchronization

SETTING	VALUE
Mode	NTP
Server	10.243.31.65, local clock as fallback
NTP authentication	off
Serves time to	both FTD units (through sftunnel)

7.1.8 VMware Tools

VMware Tools: enabled.

Other FMC system settings: REST API on (token 30 min); login banner empty; STIG and Common Criteria modes off; SecureX, AI assistant and policy analyzer off; Cisco Success Network on; geolocation updates automatic, weekly; external LDAP and RADIUS authentication not configured.

7.2 USERS

7.2.1 User Roles

ROLE	TYPE
Access Admin	system
Administrator	system
Discovery Admin	system
External Database User	system
Intrusion Admin	system
Maintenance User	system
Network Admin	system
Passive Identity User	system
Security Analyst	system
Security Analyst (Read Only)	system
Security Approver	system
Threat Intelligence Director (TID) User	system
Org read only	custom: object manager, devices, NAT, packet tracer, troubleshooting, policy submit and approve

Web login is by SAML single sign-on through Microsoft Entra ID. The IdP attribute `roles` maps "Administrator" to Administrator and "RO" to Security Analyst (Read Only); users without a mapped role receive Security Analyst (Read Only). Session timeout 180 min.

7.2.2 Users

ACCOUNT	ORGANISATION	AUTHENTICATION	ROLES (FMC USER)	SSO MAPPED ROLE
admin	local	local password	Administrator	
orgadmin	local	local password	Administrator, shell access	
Y-1	Y corp	SSO (SAML, Entra)	Administrator	Administrator
Y-2	Y corp	SSO (SAML, Entra)	Org read only, Security Analyst (Read Only), Security Approver	Security Analyst (Read Only)
Y-3	Y corp	SSO (SAML, Entra)	Org read only, Security Analyst (Read Only), Security Approver	Security Analyst (Read Only)
Y-4	Y corp	SSO (SAML, Entra)	Administrator	Administrator
Y-5	Y corp	SSO (SAML, Entra)	Administrator	Administrator
Y-6	Y corp	SSO (SAML, Entra)	Administrator	Administrator
X-1	integrator	SSO (SAML, Entra)	Administrator	Administrator
X-2	integrator	SSO (SAML, Entra)	Administrator	Administrator
X-3	integrator	SSO (SAML, Entra)	Administrator	Administrator
X-4	integrator	SSO (SAML, Entra)	Administrator	Administrator
X-5	integrator	SSO (SAML, Entra)	Administrator	Administrator

16 further accounts are internal system accounts of the FMC (for example `csn_processes`, `SRU`, `report`) and are not used for login.

8 Configuration Backup

SCHEDULED TASK (FMC)	TYPE	SCHEDULE (UTC, AS STORED)	LAST RUN SEEN
Weekly config only backup	FMC configuration backup	Monday, 02:00	2026-09-14 02:00 (source of this document)
FTD-Device-Backup	device backup, both units	Saturday, 16:00	2026-09-12 16:00 (source of this document)
Automatic SRU Imports	intrusion rule update	daily, 04:10	
Automatic Geolocation Updates	geolocation update	Saturday, 18:00	
Weekly Software Download	download latest updates	Sunday, 02:15	

No remote storage for backups is defined in the FMC configuration. The FMC also keeps a configuration snapshot of the device for each deployment (eleven kept, 2026-08-28 to 2026-09-10) and runs a daily purge job at 02:00.

Appendix A Referenced Objects by Function

Every network object referenced by the access rules, NAT, VPN and routing (369 objects), with its value from the FMC. Each object is listed once, under the first function that uses it, in document order: access rule categories, NAT, VPN topologies, routing. Group members follow their group.

Access rules: Inside-Rules (6)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
VPN_access_ALL	Group	VPN_access_clients, VPN_access_clients_admin	Internet-out
VPN_access_clients	Network	10.107.112.0/22	S2SVPN-LIC, S2SVPN-PartnerF, DMZ_rules, Internet-out, NAT exemption, VPN PartnerF, VPN HQ_LIC
VPN_access_clients_admin	Network	10.183.106.0/24	S2SVPN-SiteT, S2SVPN-SiteN, DMZ_rules, Internet-out
Internal-GUEST	Network	192.168.204.0/23	Internet-out, NAT reflection
Web-Server-HTTP	Host	10.243.31.237	INTERNET-IN-Rules, NAT Publication, NAT reflection
Fortinet_Loopback4	Host	100.91.136.183	

Access rules: INTERNET-IN-Rules (16)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
Fortinet_Loopback1	Host	100.91.136.50	Internet-out, NAT Publication, NAT auto NAT
Fortinet_Loopback2	Host	100.91.136.197	NAT Publication
Fortinet_Loopback3	Host	100.91.136.221	NAT Publication
Fortinet_Loopback7	Host	100.91.136.104	NAT Publication
Fortinet_Loopback8	Host	100.91.136.193	NAT Publication
Fortinet_Loopback9	Host	100.91.136.236	NAT Publication
SAP_host_01	Host	243.104.98.185	
SAP_host_02	Host	246.211.55.226	
SAP_host_03	Host	241.157.26.165	

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
SAP_host_04	Host	245.114.168.107	
hrgw.partner-g.example	Host	241.188.246.146	
host_03	Host	247.18.6.154	
Partner_A_NonProd_IP	Host	240.92.98.239	
host_04	Host	240.194.251.14	
sftp_43	Host	172.31.221.195	NAT Publication
IDP_VIP	Host	10.230.134.77	DMZ_rules, NAT Publication

Access rules: S2SVPN-INTEGRATOR (9)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
INTEGRATOR_Office_NET	Network	172.21.210.0/24	VPN INTEGRATOR-support
FAZ	Host	10.147.50.121	
core_sw	Host	10.147.50.24	
host_05	Host	10.147.50.50	S2SVPN-SiteN, NAT exemption
FMCv	Host	10.147.50.139	Internet-out
FTD3105_1	Host	10.147.50.21	Internet-out
FTD3105_2	Host	10.147.50.199	Internet-out
jump_33	Host	10.34.85.197	VPN INTEGRATOR-support
jump_32	Host	10.243.31.42	S2SVPN-SiteT, S2SVPN-PartnerH, VPN PartnerH, VPN INTEGRATOR-support

Access rules: S2SVPN-GCP (7)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
h_04	Host	172.29.163.178	
app_51	Host	10.243.31.219	S2SVPN-PARTNERB
sftp_42	Host	10.243.31.212	S2SVPN-PARTNERB
app_54	Host	10.243.31.134	S2SVPN-PARTNERB
h_05	Host	172.29.163.126	
SiteM_VLAN_Juliet	Network	10.243.31.208/28	S2SVPN-PARTNERB, Internet-out
SiteM_VLAN_Kilo	Network	10.243.31.128/28	S2SVPN-PARTNERB, Internet-out

Access rules: S2SVPN-SiteT (17)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
host_network_management	Host	10.243.31.4	S2SVPN-SiteN, DMZ_rules, Internet-out
S_01	Network	10.52.18.128/26	
SiteT-FG-MGMNT-01	Host	10.136.41.82	
SiteT-FG-MGMNT-02	Host	10.136.41.232	
jump_31	Host	10.243.31.86	S2SVPN-Google, DMZ_rules, Internet-out
deploy_71	Host	10.243.31.110	

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
app_56	Host	10.243.31.22	Internet-out
mail_relay_72	Host	10.243.31.83	Internet-out
net_01	Network	172.16.78.0/24	VPN Partner-A
host_06	Host	172.25.57.245	VPN Partner-A
h_06	Host	242.106.136.248	S2SVPN-PARTNERA, VPN Partner-A
directory_21	Host	10.243.31.65	S2SVPN-Google, SiteM-GCVE, Internet-out
directory_22	Host	10.243.31.93	S2SVPN-Google, SiteM-GCVE, Internet-out
pki_73	Host	10.243.31.53	
file_74	Host	10.243.31.9	Internet-out
update_75	Host	10.243.31.88	
LIC_01	Host	10.123.186.85	S2SVPN-LIC, NAT exemption, NAT Outbound source translation, VPN HQ_LIC

Access rules: S2SVPN-LIC (16)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
LIC_DESTINATIONS	Group	LIC_01, LIC_05, LIC_06	NAT Outbound source translation
LIC_05	Host	10.111.9.12	NAT exemption, NAT Outbound source translation, VPN HQ_LIC
LIC_06	Host	192.168.228.188	NAT Outbound source translation
YC-OF1	Network	10.213.210.0/23	S2SVPN-PartnerF, Internet-out, NAT exemption, VPN HQ_LIC
YC-OF2	Network	10.70.110.0/23	S2SVPN-PartnerF, Internet-out, NAT exemption, VPN HQ_LIC
LIC_02	Host	10.27.51.133	NAT exemption, VPN HQ_LIC
LIC_03	Host	10.207.158.215	NAT exemption, VPN HQ_LIC
LIC_04	Host	10.17.235.63	NAT exemption, VPN HQ_LIC
SiteT-LIC	Group	VLAN_Delta_address, SiteT-OF	NAT Outbound source translation
IDP_WAP01	Host	10.230.134.124	DMZ_rules, NAT exemption, VPN HQ_LIC
IDP_WAP02	Host	10.230.134.192	DMZ_rules, NAT exemption, VPN HQ_LIC
Print_Server	Host	10.132.6.82	
Print-Subnets	Group	Print-Subnet1, Print-Subnet2	NAT exemption, VPN HQ_LIC
Print-Subnet1	Network	10.179.254.176/28	NAT exemption, VPN HQ_LIC
Print-Subnet2	Network	10.39.128.240/28	NAT exemption, VPN HQ_LIC
VLAN_Charlie_address	Network	172.20.189.128/25	

Access rules: S2SVPN-PartnerF (3)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
PartnerF_remote_subnet_1	Network	172.17.158.0/24	VPN PartnerF
host_07	Host	10.243.31.121	
PartnerF-RDP	Host	172.17.158.210	

Access rules: S2SVPN-PARTNERA (21)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
h_07	Host	240.155.11.161	
h_08	Host	243.113.110.199	
app_55	Host	172.25.57.245	
host_08	Host	240.155.11.161	VPN Partner-A
host_09	Host	243.113.110.199	VPN Partner-A
PARTNER-A-HOSTS	Group	PARTNER_A_ZPA_1, PARTNER_A_ZPA_2, PARTNER_A_ZPA_3, PARTNER_A_ZPA_4	
PARTNER_A_ZPA_1	Host	245.95.244.127	VPN Partner-A
PARTNER_A_ZPA_2	Host	245.46.93.238	VPN Partner-A
PARTNER_A_ZPA_3	Host	242.10.64.145	VPN Partner-A
PARTNER_A_ZPA_4	Host	243.93.21.113	VPN Partner-A
app_52	Host	172.31.221.204	VPN Partner-A
EXT_IPSEC_PEERS	Group	EXT_IPSEC_PEER_1, EXT_IPSEC_PEER_2, PARTNER_SiteC_EXT	
EXT_IPSEC_PEER_1	Host	244.10.74.239	
EXT_IPSEC_PEER_2	Host	246.159.191.23	
PARTNER_SiteC_EXT	Host	245.219.151.166	S2SVPN-PARTNERB
PARTNER_A_FW_MGMT_SRC1	Network	10.143.179.0/24	VPN Partner-A
PARTNER_A_FW_MGMT_SRC2	Host	245.192.171.224	VPN Partner-A
PARTNER_A_FW_MGMT_SRC3	Host	241.40.248.254	VPN Partner-A
PARTNER_A_FW_MGMT_SRC4	Host	247.18.249.141	VPN Partner-A
SiteM_VLAN_Mike	Network	10.243.31.176/28	
PARTNER_A_FW_MGMT_SRC5	Network	240.175.244.0/24	VPN Partner-A

Access rules: S2SVPN-PARTNERB (41)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
erp_61	Host	10.243.31.40	Internet-out
svc-cert-ha.partner-b.example	FQDN	svc-cert-ha.partner-b.example	
SiteM_VLAN_Alpha	Network	172.16.173.0/24	Internet-out, NAT exemption, VPN PARTNER_B
SiteM_VLAN_Bravo	Network	172.20.189.0/25	
erpprod.partner-b.example	Host	245.88.64.154	
Telnet_ERP_PartnerB_Prod	Host	245.88.226.9	
host_10	Host	245.61.39.211	
h_09	Host	241.77.120.73	
h_10	Host	241.77.227.107	

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
SiteM_VLAN_Echo	Network	172.19.228.0/22	Internet-out, NAT exemption, VPN PARTNER_B
host_11	Host	245.88.177.104	
svc-ext-ha.partner-b.example	FQDN	svc-ext-ha.partner-b.example	
rpc01.partner-b.example	Host	245.88.8.74	
rpc02.partner-b.example	Host	245.88.243.136	
erpalt.partner-b.example	Host	245.88.11.165	
Telnet_ERP_PartnerB_Test	Host	245.88.184.178	
PARTNER_remote	Group	PARTNER_NET_02, PARTNER_NET_03, PARTNER_NET_04, PARTNER_NET_05, PARTNER_NET_06, PARTNER_NET_07, PARTNER_NET_01, PARTNER_SiteC_EXT, PARTNER_SiteD_EXT, PARTNER_NET_08, host_12	
PARTNER_NET_02	Network	244.10.74.0/24	Internet-out
PARTNER_NET_03	Network	241.77.0.0/16	
PARTNER_NET_04	Network	245.61.0.0/16	
PARTNER_NET_05	Network	247.74.237.0/24	
PARTNER_NET_06	Network	245.219.151.0/24	
PARTNER_NET_07	Network	245.170.0.0/16	
PARTNER_NET_01	Network	245.88.0.0/16	
PARTNER_SiteD_EXT	Host	244.10.74.239	
PARTNER_NET_08	Network	245.32.68.0/24	
host_12	Host	242.35.68.24	
host_13	Host	245.88.110.247	
SiteM_VLAN_Hotel	Network	172.24.57.48/28	
fwmgmt_76	Host	10.243.31.200	
PARTNER_B_Remote	Group	net_02, net_03, net_04, net_05, net_06, net_07, n_03	
net_02	Network	245.219.151.0/24	
net_03	Network	245.88.0.0/16	
net_04	Network	242.147.0.0/16	
net_05	Network	245.61.0.0/16	
net_06	Network	241.77.0.0/16	
net_07	Network	245.170.0.0/16	
n_03	Network	240.70.116.0/24	

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
SiteM_VLAN_Charlie	Network	172.20.189.128/25	Internet-out
SiteM_VLAN_Foxtrot	Network	10.243.31.192/28	Internet-out
SiteM_Servers	Network	10.243.31.0/25	Internet-out

Access rules: S2SVPN-Google (19)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
GCP_01	Network	10.190.80.0/22	
GCP_02	Network	10.231.244.0/22	SiteM-GCVE
Google_35.199.192.0__19	Network	35.199.192.0/19	SiteM-GCVE
SiteM_ESXI-MGMT	Network	10.180.162.0/24	SiteM-GCVE, Internet-out
HCX-Local	Host	10.243.31.18	
HCX-MGMT	Group	HCX-MGMT-1, HCX-MGMT-10, HCX-MGMT-11, HCX-MGMT-12, HCX-MGMT-2, HCX-MGMT-3, HCX-MGMT-4, HCX-MGMT-5, HCX-MGMT-6, HCX-MGMT-7, HCX-MGMT-8, HCX-MGMT-9	
HCX-MGMT-1	Host	10.243.31.111	
HCX-MGMT-10	Host	10.243.31.68	
HCX-MGMT-11	Host	10.243.31.35	
HCX-MGMT-12	Host	10.243.31.14	
HCX-MGMT-2	Host	10.243.31.30	
HCX-MGMT-3	Host	10.243.31.41	
HCX-MGMT-4	Host	10.243.31.13	
HCX-MGMT-5	Host	10.243.31.75	
HCX-MGMT-6	Host	10.243.31.51	
HCX-MGMT-7	Host	10.243.31.29	
HCX-MGMT-8	Host	10.243.31.62	
HCX-MGMT-9	Host	10.243.31.89	
backup_77	Host	10.243.31.57	

Access rules: S2SVPN-SiteN (2)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
SiteN-FG-MGMNT-01	Host	10.75.51.114	
SiteN-FG-MGMNT-02	Host	10.75.51.104	

Access rules: S2SVPN-PartnerH (2)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
PartnerH-JumpServer	Host	172.18.50.118	NAT exemption, VPN PartnerH
jump_34	Host	10.14.61.171	NAT exemption, VPN PartnerH

Access rules: SiteM-GCVE (2)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
host_sftp_44	Host	10.243.31.17	
GCVE-MGMT	Network	10.135.44.0/24	

Access rules: DMZ_rules (11)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
DMZ_IDP_Proxy_Hosts	Group	IDP_NLB, IDP_WAP01, IDP_WAP02	
IDP_NLB	Host	10.230.134.77	
idp_81	Host	10.243.31.23	
idp_82	Host	10.243.31.48	
NLB-IDP	Host	10.243.31.109	
DMZ_IDP_Proxy	Network	10.230.134.0/24	NAT Outbound source translation, NAT auto NAT
one.one.one.one	Host	1.1.1.1	Internet-out
dmz_proxy_83	Host	10.230.134.48	
dmz_proxy_84	Host	10.230.134.212	
IDP_WAP	Host	10.230.134.77	
pool.ntp.org	FQDN	pool.ntp.org	

Access rules: Internet-out (124)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
Fortinet-Guest-DNS-Proxy-LO	Host	100.91.136.19	
ISP-DNS_Server_01	Host	247.70.193.9	
ISP-DNS_Server_02	Host	240.196.209.175	
sap01.partner-c.example	FQDN	sap01.partner-c.example	
sap-router-01.partner-c.example	Host	244.245.6.147	
viber.com	FQDN	viber.com	
amazonaws.com	FQDN	amazonaws.com	
sftp_41	Host	10.243.31.237	NAT Publication
ftp4.partner-d.example	Host	242.114.215.221	
sftp.partner-e.example	FQDN	sftp.partner-e.example	
SiteM_WDS_Install	Network	10.78.218.0/24	
SAP_SAP01_PC1	FQDN	sap01.partner-c.example	
Amazon_EDL	Group	edl_1_Amazon	
edl_1_Amazon	Network	52.0.252.0/22	
SiteM_Xray	Network	10.114.32.0/23	
tenant.sentinelone.net	FQDN	tenant.sentinelone.net	
portal.partner-a.example	FQDN	portal.partner-a.example	

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
sectigostore.com	FQDN	sectigostore.com	
crt.sectigo.com	FQDN	crt.comodoca.com.cdn.cloudflare.net	
SAP_SAP01_PC	FQDN	sap01.partner-c.example	
SiteM_VLAN_Golf	Network	172.26.126.0/23	VPN Partner-A
Google_DNS	Host	8.8.8.8	
Microsoft_Range_5	Network	246.20.166.0/24	
Canon_counter-FTD_MIG	Group	Network_Net_264, Network_Net_265, Network_Net_393, Network_Net_394, Network_Net_395, Network_Net_396, Network_Net_397, Network_Net_398, Network_Net_399, Network_Net_400	
Network_Net_264	FQDN	a01.ugwdevice.net	
Network_Net_265	FQDN	b01.ugwdevice.net	
Network_Net_393	FQDN	hbp-ec1l.srv.ygles.com	
Network_Net_394	FQDN	kinesis.eu-central-1.amazonaws.com	
Network_Net_395	FQDN	cognito-identity.eu-central-1.amazonaws.com	
Network_Net_396	FQDN	xxxxxxxxxxxxx-ats.iot.eu-central-1.amazonaws.com	
Network_Net_397	FQDN	rgt.srv.ygles.com	
Network_Net_398	FQDN	camapi.srv.ygles.com	
Network_Net_399	FQDN	camapi-ec1.srv.ygles.com	
Network_Net_400	FQDN	hbpm-ec1l.srv.ygles.com	
smtp.office365.com	FQDN	smtp.office365.com	
Outlook_SMTP_Server	FQDN	example-com.mail.protection.outlook.com	
sub_Microsoft-office365_Range_1	Network	52.112.0.0/14	
sub_Microsoft-office365_Range_2	Network	52.96.0.0/12	
host_itsm_85	Host	10.243.31.98	
fqdn_sts.windows.net	FQDN	sts.windows.net	
fqdn_login.microsoftonline.com	FQDN	login.microsoftonline.com	
outlook.office365.com	FQDN	outlook.office365.com	
sub_Microsoft_office365_Range_3	Network	40.96.0.0/13	
sub_Microsoft-office365_Range_4	Network	40.104.0.0/15	
Zebra.com	FQDN	www.zebra.com	
b2b.partner-d.example	Host	245.3.89.204	
host_syslog_server	Host	10.243.31.94	
nelreports-cisco	FQDN	deff.nelreports.net	
FG-MGMNT-01	Host	10.147.50.202	
FG-MGMNT-02	Host	10.147.50.93	
FG-MGMNT-03	Host	10.147.50.230	

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
FG-MGMNT-04	Host	10.147.50.27	
AKAMAI_EDL	Group	edl_1_AKAMAI, edl_2_AKAMAI, edl_4_AKAMAI, edl_5_AKAMAI, edl_6_AKAMAI, edl_3_AKAMAI, edl_7_AKAMAI	
edl_1_AKAMAI	Network	23.32.0.0/11	
edl_2_AKAMAI	Network	184.24.0.0/13	
edl_4_AKAMAI	Network	23.0.0.0/12	
edl_5_AKAMAI	Network	2.16.0.0/13	
edl_6_AKAMAI	Network	95.100.0.0/15	
edl_3_AKAMAI	Network	23.192.0.0/11	
edl_7_AKAMAI	Network	104.81.96.0/20	
PartnerA_SOAP-FTD_MIG	Group	Network_Net_371, Network_Net_369, Network_Net_370, Network_Net_367, Network_Net_368, PartnerA_SOAP_api_prod, PartnerA_SOAP_api_test	
Network_Net_371	FQDN	ha.tst.int.np.partner-a-test.example	
Network_Net_369	FQDN	ma.int.partner-a.example	
Network_Net_370	FQDN	ha.dev.int.np.partner-a-test.example	
Network_Net_367	FQDN	ma.tst.int.np.partner-a-test.example	
Network_Net_368	FQDN	ma.dev.int.np.partner-a-test.example	
PartnerA_SOAP_api_prod	FQDN	apigw.partner-a.example	
PartnerA_SOAP_api_test	FQDN	apigw.sbx.partner-a.example	
RATES_FQDN	FQDN	www.rates-service.example	
date.nager.at	FQDN	date.nager.at	
fqdn_dev.azure.com	FQDN	dev.azure.com	
app_59	Host	10.243.31.118	
api.smartsheet.eu	FQDN	api.smartsheet.eu	
api.smartsheet.com	FQDN	api.smartsheet.com	
Portal-Access_PARTNERA	Group	host_portaluatextlb.partner-a.example, host_portaluat.partner-a.example, host_portalprodextlb.partner-a.example, host_portal.partner-a.example, host_portalinternal.partner-a.example, host_portalinternaluat.partner-a.example	
host_portaluatextlb.partner-a.example	Host	243.250.160.180	
host_portaluat.partner-a.example	Host	240.255.146.250	
host_portalprodextlb.partner-a.example	Host	240.9.184.170	
host_portal.partner-a.example	Host	243.218.254.96	
host_portalinternal.partner-a.example	Host	240.187.118.93	VPN Partner-A
host_portalinternaluat.partner-a.example	Host	244.166.205.60	VPN Partner-A
app_57	Host	10.243.31.105	

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
cacerts.digicert.com	FQDN	cacerts.digicert.com	
erp_62	Host	10.243.31.20	
app_58	Host	10.243.31.101	
erp_63	Host	10.243.31.43	
sap01.partner-c.example_SAP	Host	242.123.58.215	
PartnerA-Guest	Network	192.168.129.0/24	
PartnerB-Guest	Network	192.168.145.0/24	
External-GUEST	Network	192.168.231.0/24	
SiteKOpenVPN	Host	247.50.16.251	
SiteM_VLAN_November	Network	10.25.103.0/24	
loadproof.us	FQDN	loadproof.us	
Microsoft_Office_365	Group	login.microsoftonline.com, login.microsoft.com, login.windows.net	
login.microsoftonline.com	FQDN	login.microsoftonline.com	
login.microsoft.com	FQDN	login.microsoft.com	
login.windows.net	FQDN	login.windows.net	
Google_play	FQDN	play.google.com	
h_11	Host	240.146.209.217	
h_12	Host	247.40.113.72	
YC-PRN	Network	10.251.139.0/24	
YC-IoT	Network	10.9.30.0/24	
fqdn_prusa3d.com	FQDN	prusa3d.com	
NDR_Sensor	Host	10.237.237.45	
NDR_ext_url	Group	api.ndr-vendor.example, update2.ndr-vendor.example, vpn.ndr-vendor.example, content.telemetry.ndr-vendor.example, data.telemetry.ndr-vendor.example	
api.ndr-vendor.example	FQDN	api.ndr-vendor.example	
update2.ndr-vendor.example	FQDN	update2.ndr-vendor.example	
vpn.ndr-vendor.example	FQDN	vpn.ndr-vendor.example	
content.telemetry.ndr-vendor.example	FQDN	content.telemetry.ndr-vendor.example	
data.telemetry.ndr-vendor.example	FQDN	data.telemetry.ndr-vendor.example	
sub_TS-PartnerH	Network	10.14.61.0/24	
SiteM_VLAN_India	Network	172.31.221.192/28	
SiteM_Quebec	Network	10.243.31.224/28	
sub_TS-INTEGRATOR	Network	10.34.85.0/24	
SiteM_VLAN_Lima	Network	172.25.57.240/28	
OT-Servers	Network	10.231.220.0/24	

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
ot_dns_91	Host	10.231.220.143	
ot_ntp_92	Host	10.231.220.221	
time.windows.com	FQDN	time.windows.com	
Last_hop_to_PC_SAP_router	Host	241.21.195.10	
host_dmz_proxy_83	Host	10.230.134.48	
host_dmz_proxy_84	Host	10.230.134.212	
Google_DNS_02	Host	8.8.4.4	
8.8.8.8	Host	8.8.8.8	

Access rules: Temporary rules (1)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
nw_03	Network	10.147.50.0/24	VPN INTEGRATOR-support

NAT: NAT exemption (23)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
PARTNERB_LOCAL_GROUP	Group	SiteM_VLAN_Alpha, n_02, SiteM_VLAN_Echo, nw_01	
n_02	Network	172.20.189.0/24	VPN PARTNER_B
nw_01	Network	10.243.31.0/24	VPN PARTNER_B
PARTNERB_REMOTE_GROUP	Group	net_02, net_03, net_04, net_05, net_06, net_07, n_03	
HQ_LIC_LOCAL	Group	Print_Host_01, Print_Host_02, Print_Host_03, Print_Host_04, Print_Host_05, Print_Host_06, Print_Host_07, Print_Host_08, Print_Host_09, Print_Host_10, YC-OF2, IDP_WAP02, IDP_WAP01, Print_Host_11, VPN_access_clients, Network_Net_233, YC-OF1	
Print_Host_01	Host	172.20.189.170	VPN HQ_LIC
Print_Host_02	Host	172.20.189.148	VPN HQ_LIC
Print_Host_03	Host	172.20.189.195	VPN HQ_LIC
Print_Host_04	Host	172.20.189.145	VPN HQ_LIC
Print_Host_05	Host	172.20.189.157	VPN HQ_LIC
Print_Host_06	Host	172.20.189.130	VPN HQ_LIC
Print_Host_07	Host	172.20.189.175	VPN HQ_LIC
Print_Host_08	Host	172.20.189.168	VPN HQ_LIC
Print_Host_09	Host	172.20.189.147	VPN HQ_LIC
Print_Host_10	Host	172.20.189.242	VPN HQ_LIC
Print_Host_11	Host	172.20.189.248	VPN HQ_LIC
Network_Net_233	Network	10.243.31.0/25	VPN HQ_LIC
HQ_LIC_REMOTE	Group	LIC_01, LIC_04, LIC_05, LIC_03, nw_04, LIC_02, Print-Subnets	
nw_04	Host	10.132.6.82	VPN HQ_LIC

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
SiteN_S2SLocal	Group	host_05	
SiteT_S2SLocal	Group	Tango, SiteM_NW-MGMT, h_13	
SiteM_NW-MGMT	Network	10.147.50.0/24	
h_13	Host	242.106.136.248	

NAT: Outbound source translation (8)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
LIC_outbound_PAT	Host	10.243.31.59	
Kilo_VLAN_keepalive_IP	Host	10.243.31.136	
Intermediate_Server	Host	172.29.163.178	
Fortinet_Transit_IF_Alias	Host	100.91.136.59	
Juliet_VLAN_keepalive_IP	Host	10.243.31.216	
Fortinet_Server_IF_IP	Host	10.243.31.100	
SiteT_Meraki_IF	Host	172.16.78.199	
SiteT_Meraki_Papa_IF	Host	10.52.18.179	

NAT: Publication (8)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
PARENT-HQ-IT	Group	Parent_HQ_public_IP_1, Parent_HQ_public_IP_2, Parent_HQ_public_IP_3	
Parent_HQ_public_IP_1	Host	241.237.53.137	
Parent_HQ_public_IP_2	Host	242.198.45.198	
Parent_HQ_public_IP_3	Host	247.79.82.20	
Public_IP_4	Host	247.222.237.2	
IDP-PUBLIC	Host	247.222.237.3	NAT auto NAT
Public_IP_2	Host	247.222.237.5	NAT reflection
Public_IP_3	Host	247.222.237.6	

VPN: PartnerF (3)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
PartnerF_local_subnet_1	Network	10.243.31.0/24	
Victor	Network	10.70.110.0/23	
Uniform	Network	10.213.210.0/23	

VPN: Partner-A (3)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
app_53	Host	172.31.221.201	
host_01	Host	244.10.74.239	
host_02	Host	246.159.191.23	

VPN: PARTNER_B (1)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
Clean_WiFi	Network	10.233.16.0/22	

VPN: HQ_GCP (3)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
Network_Net_210	Network	10.243.31.128/28	
Network_Net_206	Network	10.243.31.208/28	
net_08	Network	172.29.163.0/24	

Routing (23)

OBJECT	TYPE	VALUE / MEMBERS	ALSO USED IN
isp-wan-gw	Host	247.222.237.4	
IPv4-Private-All-RFC1918	system	10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16	
Fortinet_Loopbacks	Network	100.91.136.0/24	S2SVPN-GCP
Fortinet-transit	Host	10.243.31.246	Internet-out, NAT Outbound source translation, NAT auto NAT
PARTNER-EXT-FW_Loopback	Host	245.141.92.205	S2SVPN-PARTNERB
PARTNER-EXT-FW_Address	Host	10.243.31.186	S2SVPN-PARTNERA, S2SVPN-PARTNERB, VPN Partner-A
PARTNER_Public_Services	Group	static_other_public_3, static_other_public_2, partnera.portal_2, partnera.portal_1	NAT Outbound source translation
static_other_public_3	Network	245.88.176.0/23	NAT Outbound source translation
static_other_public_2	Host	245.88.200.228	NAT Outbound source translation
partnera.portal_2	Host	246.121.155.26	NAT Outbound source translation
partnera.portal_1	Host	247.196.136.228	NAT Outbound source translation
SiteN_S2SRemote	Group	SiteN-NW-MGMT	NAT exemption
SiteN-NW-MGMT	Network	10.75.51.0/24	S2SVPN-SiteN, NAT exemption
SiteT_S2SRemote	Group	SiteT-PRN, SiteT-OF, SiteT-NW-MGMT, VLAN_Delta_address	S2SVPN-SiteT, NAT exemption
SiteT-PRN	Network	10.94.108.0/24	S2SVPN-SiteT, NAT exemption
SiteT-OF	Network	10.243.158.0/24	S2SVPN-SiteT, S2SVPN-LIC, NAT exemption, NAT Outbound source translation
SiteT-NW-MGMT	Network	10.136.41.0/24	S2SVPN-SiteT, NAT exemption
VLAN_Delta_address	Network	172.16.78.0/24	S2SVPN-SiteT, S2SVPN-LIC, S2SVPN-PARTNERA, NAT exemption, NAT Outbound source translation
Tango	Network	10.243.31.0/25	S2SVPN-SiteN, NAT exemption
static_remote_SiteM_ESXI-MGMT	Network	10.180.162.0/24	
static_remote_Test_vMotion	Network	10.154.21.0/24	S2SVPN-Google
SiteM_vMotion	Network	10.114.102.0/24	SiteM-GCVE
SiteM_ESXI-GCE-Uplink	Network	10.229.126.0/24	SiteM-GCVE

Appendix B Referenced Port Objects

Every port object and port group referenced by the access rules and NAT (89 objects), with its value from the FMC. Groups show their members resolved to protocol and port. Cisco predefined objects are marked as predefined.

OBJECT	TYPE	VALUE
custom-14	ProtocolPort	TCP (6)/custom-14
custom-02	ProtocolPort	TCP (6)/custom-02
custom-01	ProtocolPort	TCP (6)/custom-01
8080	ProtocolPort	TCP (6)/8080
8888	Group	TCP (6)/8888, UDP (17)/8888
8889	Group	TCP (6)/8889, UDP (17)/8889
custom-13	ProtocolPort	TCP (6)/custom-13
ALL_ICMP	ICMPV4	ICMP (1)
PartnerF-rdp-service	ProtocolPort	TCP (6)/custom-09
Canon-remote-operation-ports	Group	TCP (6)/5900, TCP (6)/custom-26
CAPWAP	ProtocolPort	UDP (17)/5246-5247
Carbonite_Double_Take	Group	TCP (6)/6320, TCP (6)/6325
DamewareMRC	ProtocolPort	TCP (6)/6129
DCE-RPC	Group	TCP (6)/135, TCP (6)/5001-5100, TCP (6)/445, TCP (6)/593, TCP (6)/1024-5000, TCP (6)/49152-65535, UDP (17)/135
DNS	Group	TCP (6)/53, UDP (17)/53
DNS_over_TCP	ProtocolPort (predefined)	TCP (6)/53
DNS_over_UDP	ProtocolPort (predefined)	UDP (17)/53
ESP_	ProtocolPort	ESP (50)
VPN_access	ProtocolPort	TCP (6)/custom-20
VPN_access2	ProtocolPort	TCP (6)/custom-21
VPN_access_ipsec	ProtocolPort	UDP (17)/custom-04
VPN_access_ipsec_HQIT	ProtocolPort	UDP (17)/custom-05
VPN_access_HQIT	ProtocolPort	TCP (6)/custom-22
HTTP	ProtocolPort (predefined)	TCP (6)/80
HTTPS	ProtocolPort (predefined)	TCP (6)/443
HTTPS-only443	ProtocolPort	TCP (6)/443
icmp_req	ICMPV4	ICMP (1)/8
IKE	Group	UDP (17)/500, UDP (17)/4500

OBJECT	TYPE	VALUE
IMAPS	ProtocolPort	TCP (6)/993
IPSEC-NAT-Traversal	Group	TCP (6)/100-65000, UDP (17)/100-65000
LIC	ProtocolPort	TCP (6)/1688
LINEmessenger	Group	TCP (6)/5223, TCP (6)/5242, TCP (6)/9418, TCP (6)/10000-10020, UDP (17)/5223, UDP (17)/5242, UDP (17)/9418, UDP (17)/10000-10020
NTP	Group	TCP (6)/123, UDP (17)/123
OPENVPN	Group	TCP (6)/1194-1195, UDP (17)/1194-1195
PDQ	Group	TCP (6)/6336, TCP (6)/7337, TCP (6)/445, TCP (6)/139
PING	ICMPV4	ICMP (1)/8
Printer-webmgmt	ProtocolPort	TCP (6)/8000
Printing	Group	TCP (6)/9100-9102, TCP (6)/515, TCP (6)/8000, TCP (6)/8080, TCP (6)/80, TCP (6)/443, TCP (6)/8443, TCP (6)/custom-27, TCP (6)/custom-28, UDP (17)/427
RCP	ProtocolPort	TCP (6)/135
RDP	ProtocolPort	TCP (6)/3389
RDP_UDP	ProtocolPort	UDP (17)/3389
SAP_sap01_pc	Group	TCP (6)/3299, TCP (6)/custom-29
SAP_sap01_pc2	Group	TCP (6)/3299, TCP (6)/custom-29
SAP_SAP01_PC_ports	Group	TCP (6)/3299, TCP (6)/custom-30
SAP_SAP01_PC_ports_tcp_3299	ProtocolPort	TCP (6)/3299
SAP_prod_router_pc	ProtocolPort	TCP (6)/custom-19
SAP_tcp_3299	ProtocolPort	TCP (6)/3299
SFTP_alt_port	ProtocolPort	TCP (6)/custom-23
Portal-Access-PartnerA-LB	ProtocolPort	TCP (6)/8883
Portal-Access-PartnerA-UA	ProtocolPort	TCP (6)/custom-18
SMB	ProtocolPort	TCP (6)/445
SMTP	ProtocolPort (predefined)	TCP (6)/25
SMTP-TX	ProtocolPort	TCP (6)/587
SNMP_tcp_161-162	ProtocolPort	TCP (6)/161-162
SNMP_UDP	ProtocolPort	UDP (17)/161-162
SNMP_udp_161-162	ProtocolPort	UDP (17)/161-162
SSH	ProtocolPort (predefined)	TCP (6)/22
TCP_custom-11	ProtocolPort	TCP (6)/custom-11
TCP9100	ProtocolPort	TCP (6)/9100
TCP_custom-24	ProtocolPort	TCP (6)/custom-24
TCP_custom-06	ProtocolPort	TCP (6)/custom-06
TCP_custom-16	ProtocolPort	TCP (6)/custom-16

OBJECT	TYPE	VALUE
TCP_custom-02_2	ProtocolPort	TCP (6)/custom-02
TCP_custom-01_1	ProtocolPort	TCP (6)/custom-01
TCP_custom-01_2	ProtocolPort	TCP (6)/custom-01
TCP_49	ProtocolPort	TCP (6)/49
TCP_514	ProtocolPort	TCP (6)/514
TCP_541	ProtocolPort	TCP (6)/541
TCP_custom-17	ProtocolPort	TCP (6)/custom-17
TCP_custom-07	ProtocolPort	TCP (6)/custom-07
TCP_custom-15	ProtocolPort	TCP (6)/custom-15
TCP_8080	ProtocolPort	TCP (6)/8080
TCP_custom-08	ProtocolPort	TCP (6)/custom-08
TCP_84431	ProtocolPort	TCP (6)/8443
TCP_8890	ProtocolPort	TCP (6)/8890
TCP_custom-10	ProtocolPort	TCP (6)/custom-10
TCP_9100	ProtocolPort	TCP (6)/9100
TCP_custom-13	ProtocolPort	TCP (6)/custom-13
UDP9443	ProtocolPort	UDP (17)/9443
UDP_123	ProtocolPort	UDP (17)/123
UDP_custom-12	ProtocolPort	UDP (17)/custom-12
UDP_21116	ProtocolPort	UDP (17)/21116
UDP_514	ProtocolPort	UDP (17)/514
viber-ports	Group	UDP (17)/5243, UDP (17)/7985, TCP (6)/7985, UDP (17)/5242, TCP (6)/5243, TCP (6)/4244, TCP (6)/5242, UDP (17)/4244
VodaFemtoCell	Group	ESP (50), TCP (6)/123, UDP (17)/123, UDP (17)/500, UDP (17)/4500, ICMP (1), TCP (6)/53, UDP (17)/53, TCP (6)/80, TCP (6)/443
Windows_AD	Group	TCP (6)/135, TCP (6)/5001-5100, TCP (6)/445, TCP (6)/593, TCP (6)/1024-5000, TCP (6)/49152-65535, UDP (17)/135, TCP (6)/53, UDP (17)/53, TCP (6)/88, TCP (6)/464, UDP (17)/88, UDP (17)/464, TCP (6)/389, UDP (17)/389, TCP (6)/139, TCP (6)/445, TCP (6)/3268-3269, TCP (6)/636, TCP (6)/636, UDP (17)/123
WSUS_PORTS	ProtocolPort	TCP (6)/8530-8531
WSUS_PORTS_2	Group	TCP (6)/custom-31, TCP (6)/custom-32, TCP (6)/custom-33
NetMgmt	ProtocolPort	TCP (6)/10050-10051

About this version

This document was produced for its owner from the device and Management Center backups, and is published here as a sample of the work. To publish it, these classes of value were substituted, consistently, one replacement per original throughout:

CLASS	IN THIS VERSION
The corporate domain, every host name built on it, the mail domain	example.com, FW3105-1 and FW3105-2
Server names	named by role and renumbered: directory_21, jump_31, network_management, syslog_server and so on
Site, building, network and application names inside zone, rule, VPN and object names	neutral names: sites and buildings as Site and a letter, network segments from the phonetic alphabet (SiteM_VLAN_Alpha), IDP, LIC, NetMgmt, NDR
Object names built from an address	numbered: h_01, net_01, PARTNER_NET_01 and so on
VLAN and subinterface numbers	other numbers, the same everywhere
Chassis serial numbers, and the unit part of each MAC address	withheld
The organisation's business partners, their domains, host names and sites	Partner A to Partner H, partner-a.example and so on
The vendor of the internal firewall and of its remote access VPN, and the MFA provider	Fortinet, VPN_access, Entra
Anything that places the organisation in a country or a town: the ISP, the time zone, a local service, local spellings in object names	ISP, Local, rates-service.example
Every public IPv4 address, except the published ranges of generic vendors	addresses from 240.0.0.0/4, which is reserved and never routed
Every private, shared and link-local address	another address from the same range
Port numbers that are not the registered or published default for their service	withheld, shown as custom-01, custom-02 and so on
Administrator accounts, the integrator's name and the organisation's own prefixes	role labels, Y-1 to Y-6 and X-1 to X-5; YC-

Everything else is exactly as the device and the Management Center hold it: every model and software version of the perimeter pair and its management centre, every count, rule, object and table, the standard service ports, and the published address ranges of generic vendors (Microsoft, Google, Amazon, Akamai) where the configuration pins them; one regional range is substituted like any other public address.

Each original value has one replacement, used everywhere it appears, and every host still sits in the same networks it sits in on the device, so a peer can be followed from its VPN topology to its access rules and its NAT exemption. The substituted addresses are not live: 240.0.0.0/4 is reserved and never routed on the Internet.

References

DOCUMENT	CONTENT
FTD-Device-Backup_FW3105-1_Primary_20260912160002.tar	FTD device backup, primary unit
Weekly_config_only_backup_20260914020001	FMC configuration backup
Cisco Secure Firewall Management Center Device Configuration Guide, 7.6	FTD configuration reference
Cisco Secure Firewall Management Center Administration Guide, 7.6	FMC system configuration reference
Documentation template supplied by the organisation	chapter structure of this document