Getting Started

Choose the Right Migration Process

There are three methods to migrate Adaptive Security Appliance (ASA) configurations to Firepower Threat Defense (FTD) devices:

- CDO solution—If you intend to migrate your ASA configurations to FTD devices and manage them with Cisco Defense Orchestrator (CDO) and Firepower Device Manager (FDM), use the cloud-based process in CDO to migrate your ASA configurations.
- On-Premise solution (FMC)—If you intend to migrate your ASA configurations to FTD devices and manage them with Firepower Management Center (FMC), use the desktop application method to migrate your ASA configurations.

  To download the latest version of the Firepower Migration Tool, browse to https://software.cisco.com/download/home/286306503/type and click Firepower Migration Tool.

  You can also download the Migration Tool from the Firepower Threat Defense device download page.
- On-Premise solution (FDM)—If you intend to migrate your ASA configurations to FTD devices and manage them with Firepower Device Manager (FDM), use the cloud-based process in CDO to migrate your ASA configurations. You can then use FDM to manage your configuration.

This guide assumes that you have a basic understanding of CDO operations. To learn more, see the CDO Data Sheet.

About the Cisco Defense Orchestrator Migration Process

CDO can help you migrate your Adaptive Security Appliance (ASA) to a Firepower Threat Defense (FTD) device. CDO provides a wizard to help you migrate these elements of the ASA's running configuration to an FTD template:

- Interfaces
- Routes
- Access Control Rules (ACLs)
- Network Address Translation (NAT) rules
- Network objects and network group objects

Note CDO does not support object names with reserved keywords. Rename the object names by adding a suffix "ftdmig" to it.

- Service objects and service group objects
- Site-to-Site VPN

Note Any unreferenced object or object-groups in the configuration will be dropped, and marked as unused during the migration.

Once these elements of the ASA running configuration have been migrated to an FTD template, you can then apply the FTD template to a new FTD device that is managed by CDO. The FTD device adopts the configurations defined in the template, and so, the FTD is now configured with some aspects of the ASA's running configuration.

Other elements of the ASA running configuration are not migrated using this process. Those other elements are represented in the FTD template by empty values. When the template is applied to an FTD, we apply values we migrated to the new FTD and ignore the empty values. Whatever other default values the new FTD has, it retains. Those other elements of the ASA running configuration that we did not migrate, will need to be recreated on the FTD outside the migration process.

License for the Migration Process

The Firepower Migration process is part of CDO and does not require any specific license other than the CDO license.

Guidelines and Limitations

Note Configurations that are not supported in CDO will be dropped during migration as **Unsupported** and will be reported in the **Migration Report**.

Feature or Function Name	What Can be Migrated	Restrictions or Limitations of Migration
Firewall Modes	Routed firewall mode	Transparent mode configurations cannot be migrated.

Interface Configurations	• Physical interfaces
	• Subinterfaces
		• The FTD must have equal or more physical interfaces than the ASA interface configurations being migrated.
		• Subinterfaces (subinterface ID will always be set to the same number as the VLAN ID on migration)
		• The following interface configurations will not be migrated to FTD:
		  • Secondary VLANs on ASA interfaces
		  • Port channel
		  • Redundant Interface
		  • Bridge Group Interface
		  • Virtual Tunnel Interface

Routing	Static routes	• When there are multiple static routes with the same network as destination, only one route with minimum metric value is migrated and others are dropped.
		• The following route features will not be migrated to FTD:
		  • Tunneled routes
		  • Null 0 interface routes
		  • Static routes with SLA track

Feature or Function Name	What Can be Migrated	Restrictions or Limitations of Migration
Access Control Rules (ACLs)	• Enabled Access Control Rules • Source and destination objects • CDO supports actions like Allow, Trust, and Block for FTD. During the migration, permit and deny actions in the source ASA configuration are handled and are mapped to the supported action for FTD on CDO. • CDO supports migration of ACLs attached to a policy, interface, or an access group without an IP protocol. • ACE with unencrypted L3 Tunnel protocols	The following ACL features will not be migrated to FTD: • CDO and FDM do not support ACL with IPv4 and IPv6 mixed protocols • Logging severity-level information • Inactive or disabled rules • ACE with service object or service group having non-TCP, UDP, or ICMP protocols • ACE with non-TCP or UDP service objects • Non-TCP or UDP protocol in ACE with inline objects • ACEs with Time-range • Access list not mapped with access group
Network Address Translation (NAT) Rules	• Network Object (Auto) and twice (Manual) NAT or PAT • Static NAT • Dynamic NAT or PAT • Identity NAT • Source Port (service) Translation	The following NAT rules features will not be migrated to FTD: • PAT pool • Unidirectional • Inactive • With Twice NAT, the use of **destination** service objects for destination port (service) translation (including service objects that have both the source and destination) • Destination port translation • NAT46, NAT64 **Note** CDO does not support network object with 0.0.0.0/32.

Feature or Function Name	What Can be Migrated	Restrictions or Limitations of Migration
Service Objects and Service Group Objects	Service Objects and Nested Groups See Supported IP Protocols on CDO for the list of protocols used in services objects that CDO supports.	• The protocols, BCC-RCC-MON, and BBN-RCC-MON, are not supported. • Operators like less than, greater than, and not equal to, are not supported. • Object-group nesting
Network Objects and Network Group Objects	Network Objects and Network Group Objects	The following network object or network group are unsupported: • Discontinuous Mask Based • IP address starting with first octet ‘0’ in IPv4 address
ICMP Types	ICMP Types	The following ICMP types are unsupported: • ICMP–based service object entries with INVALID ICMP type or/and code • Service–type or ICMP–type object without code for ICMPv4 or ICMPv6 type • Any unassigned ICMP type (as per IANA) or Invalid ICMP type
Miscellaneous Unsupported Objects	-	The following miscellaneous objects are unsupported: • SGT–based Network Object-Group • User–based Network Object-Group

Feature or Function Name	What Can be Migrated	Restrictions or Limitations of Migration
Site-to-Site VPN	• Phase 1 and Phase 2 proposals for both IKEv1 and IKEv2 • Perfect Forward Secrecy (PFS) for both IKEv1 and IKEv2 • Crypto Access List with Nested Object-Group • Crypto Map with multiple peer IPs • Both IKEv1 and IKEv2 used for a tunnel in Crypto Map	The following Site-to-Site VPN features are not supported: • VPN-Filter • vpn-idle-timeout • isakmp keepalive threshold 10 retry 10 • Crypto Map VPNMAP 200 set security-association lifetime seconds 360 • set security-association lifetime kilobytes unlimited • set security-association lifetime seconds 3600 • Certificate Authentication • Dynamic Crypto Map • Route–based VPN (virtual tunnel interface)

Note Remote Access VPN is completely unsupported.

For more information on Guidelines and Limitations, see Guidelines and Limitations for ASA Configurations and Guidelines and Limitations for Firepower Threat Defense Devices.

Supported IP Protocols on CDO

The IP Protocols that CDO supports in service objects are as follows:

IP Protocols in Service Objects			
1= ICMP	34 = THREEPC	73 = CPHB	106= QNX
2 = IGMP	35 = IDPR	74 = WSN	107 = AN
3 = GGP	36 = XTP	75 = PVP	108 = IPCOMP
5 = ST2	37 = DDP	76 = BRSATMON	109= SNP
6 = TCP	38 = IDPRCMTP	78 = WBMON	110 = COMPAQPEER
7 = CBT	39 = TPPLUSPLUS	77 = SUNND	111 = IPXINIP
8 = EGP	40 = IL	79 = WBEXPAK	112 = VRRP
9 = IGP	42 = SDRP	80 = ISOIP	113= PGM
10 = BBNRCCMON	45 = IDRP	81 = VMTP	115 = L2TP
11 = NVP2	46 = RSVP	82 = SECUREVMTP	116 = DDX
12 = PUP	48 = MHRP	83 = VINES	117= IATP
13 = ARGUS	49 = BNA	84 = TTP	118 = ST
14 = EMCON	50 = ESP	85 = NSFNETIGP	119= SRP
15=XNET	51 = AH	86 = DGP	120= UTI
16 = CHAOS	52 = INLSP	87 = TCF	121= SMP
17 = UDP	53 = SWIPE	88 = EIGRP	122= SM
18 = MUX	54 = NARP	89 = OSPFIGP	123= PTP
19 = DCNMEAS	55 = MOBILE	90 = SPRITERPC	124= ISIS
20 = HMP	56 = TLSP	91 = LARP	125 = FIRE
21 = PRM	57 = SKIP	92 = MTP	126 = CRTP
22 = XNSIDP	58= IPv6-ICMP	93 = AX25	127 = CRUDP
23 = TRUNK1	59 = IPv6NONXT	94 = IPIP	128 = SSCOPMCE
24 = TRUNK2	62 = CFTP	95 = MICP	129 = IPLT
25 = LEAF1	64 = SATEXPAK	96 = SCCSP	130= SPS
26 = LEAF2	65 = KRYPTOLAN	97 = ETHERIP	131= PIPE
27 = RDP	66 = RVD	98 = ENCAP	132 = SCTP
28 = IRTP	67 = IPPC	100 = GMTP	133 = FC
29 = ISOTP4	69 = SATMON	101 = IFMPP	254 = DIVERT
30 = NETBLT	70 = VISA	102= PNNI	
31 = MFENSP	71 = IPCV	103= PIM	
32 = MERITINP	72 = CPNX	104 = ARIS	
33 = SEP		105= SCPS	

Best Practices

Follow these best practices when using CDO to migrate an ASA configuration to an FTD template:

- Ensure you fetch the running configuration from an ASA device using **show run** command in a model device migration.
- Review the migration reports for skipped, unsupported, and partially supported configurations.
- After migration, verify the migrated rules and objects in the FTD template before deploying it to an FTD.
- Optimize your ASA policies before migrating them to an FTD template.
- We recommend that you deploy the migrated ASA configuration to an FTD device that does not have an existing configuration.