The Cisco AI Assistant is now available to try out for network management, troubleshooting, and monitoring use cases. Sign up to the controlled availability on the Early Access page. You will be added to the waitlist and notified when your Org is enabled. Read more.

Firewall

Layer 3

Inbound rules

#	Policy	Rule description	Protocol	Source	Src port	Destination	Dst port	Syslog	Enforce	Actions
		No custom rules defined								
	Deny	Default rule	Any	Any	Any	Any	Any			

Outbound rules

#	Policy	Rule description	Protocol	Source	Src port	Destination	Dst port	Syslog	IPv4 hits	Enforce	Actions
40	Allow	Office365	TCP	Data	Any	52.244.207.172/32 52.244.223.198/32 52.247.150.191/32 1.80.125.22/32 13.91.91.243/32 13.107.6.156/31 13.107.7.190/31 13.107.9.156/31 40.81.156.154/32 40.90.218.198/32 52.108.0.0/14 52.174.56.180/32 52.183.75.62/32 52.184.165.82/32 104.42.230.91/32 157.55.145.0/25 157.55.155.0/25 157.55.227.192/26 20.190.128.0/18 40.126.0.0/18 13.107.64.0/18 52.112.0.0/14 52.120.0.0/14 52.238.119.141/32 52.244.160.207/32	80,443	0		
41	Deny		Any	Scanner	Any	Any	Any	0			
42	Allow	IOT Internet Access	TCP	IoT	Any	Any	80,443	0			
43	Allow	Allow NTP Access for IOT	UDP	IoT	Any	pool.ntp.org	123	0			
44	Allow	Polycom Windows NTP	UDP	Voice	Any	Windows NTP Server IP	123	0			
45	Allow	Polycom SIP SSL/5061	TCP	Voice	Any	MS Teams Media IPs	5061	0			
46	Allow	Polycom TCP/49152	TCP	Voice	Any	MS Teams Media IPs	49152	0			
47	Allow	Polycom UDP/3478-3481	UDP	Voice	Any	MS Teams Media IPs	3478-3481	0			
48	Allow	Polycom RTP and RTCP	UDP	Voice	Any	MS Teams Media IPs	49152-53247	0			
49	Allow	Polycom Google Services	TCP	Voice	Any	Google_AndroidClients Google_ClientServices Google_FireBaseRemoteConfig Google_MTalk	5228	0			
	Allow	Default rule	Any	Any	Any	Any	Any	0			

Cellular failover rules ☐ Cellular failover rules apply to Cellular and WAN 2

#	Policy	Rule description	Protocol	Source	Src port	Destination	Dst port	Syslog	Enforce	Actions
1	Deny	Deny guest over MPLS link	Any	Guest	Any	Any	Any			
	Allow	Default rule	Any	Any	Any	Any	Any			

Inbound cellular failover rules

#	Policy	Rule description	Protocol	Source	Src port	Destination	Dst port	Syslog	Enforce	Actions
		No custom rules defined								
	Deny	Default rule	Any	Any	Any	Any	Any			

WAN appliance services

Service	Allowed remote IPs
ICMP ping	184.183.25.158, 209.180.150.55, 70.190.113.130, 76.220.127.88
Web (local status & configuration)	None
SNMP	None

Layer 7

Firewall rules: There are no rules defined for this network.
Add a layer 7 firewall rule

Forwarding rules

Port forwarding: There are no port forwarding rules on this network.
Add a port forwarding rule

1:1 NAT: There are no 1:1 NAT mappings.
Add a 1:1 NAT mapping

1:Many NAT: There are no 1:Many NAT mappings.
Add 1:Many IP

Bonjour forwarding

Rules: There are no Bonjour forwarding rules on this network.
Add a Bonjour forwarding rule

IP source address spoofing protection

Mode: Log

This network is *not* protected from IP spoofing. For more information, see this KB article and this IETF recommendation.