SECURITY AND PRIVACY WHITE PAPER

Firewall Traversal for Video Conferencing with Polycom RealPresence DMA 10.x

Part 3725-86421-001

Version 02

March 2020

Introduction

This white paper addresses security and privacy related information regarding Firewall Traversal for Video Conferencing with the Polycom RealPresence Distributed Media Application (DMA) 10.x. This white paper is supplemental to the Poly Privacy Policy. The most current version of this white paper will be available on Poly's website.

DMA is a network-based software application that manages and distributes calls across collaboration networks. This white paper specifically addresses the edge configuration option.

You may configure each system with a core configuration, an edge configuration, or a combination thereof. The Polycom RealPresence DMA system in edge configuration provides NAT and firewall traversal for video conferencing media (specifically, SIP, H.323, audio stream, video stream, content stream, WebRTC, LDAP, XMPP, HTTPS). The DMA in edge configuration is meant to be installed behind an organization's firewall to act as a single point of entry/exit for communication between internal video endpoints and the outside world. The DMA can facilitate connections between the organization's internal network and external networks, including cloud services. This can enable an organization to connect to cloud services, such as remotely hosted virtual meeting rooms and collaboration, in conjunction with local, on-premises video endpoints, while still maintaining a secure network. The DMA may be on-premise or installed in the cloud (Amazon AWS, Microsoft Azure).

Because a DMA system communicates with an organization's internal network and the outside world, the system must have certain firewall ports opened. It then acts as an intermediary, sending all signaling and media traffic between the intranet and external networks. In this configuration, individual endpoints within the organization's network remain isolated and protected against intrusion from the outside world by the firewall and the DMA.

DMA deployments

When you install one or more RealPresence DMA systems, you need to configure each system with a core configuration, an edge configuration, or a combination configuration as follows:

1. A core configuration is recommended if the system(s) is deployed inside your network environment.
2. An edge configuration provides additional security features (see Access Control Lists and Security and Redundancy) and is recommended if you deploy the system in the DMZ and it communicates with one or more core-configured systems inside your enterprise network.
3. A combination system is one of the following:
   - an edge-configured system that resides in the DMZ and does not communicate with any core configured system, or
   - an edge-configured system inside the enterprise that is part of a VPN tunnel and does not communicate with any core configured system

DMA ports summary

A DMA can be configured in different ways, with a variety of services enabled or disabled. There are some differences between the default port configurations on a freshly-installed RealPresence Access Director (RPAD) system versus a freshly-installed DMA in edge configuration system. Additionally, a DMA upgraded from an RPAD system will have different port configurations than a freshly-installed DMA. The upgraded DMA system will have the same port ranges that were configured in the original RPAD system. The *RealPresence Distributed Media Application (DMA) System Security and Privacy Guide* provides a complete list of all ports that are required to be opened on internal and external firewalls for specific services.

Application -Level Gateways

Using an Application-Level Gateway (ALG) in conjunction with a DMA is not recommended. The DMA in edge configuration performs the same tasks as an ALG and properly handles the protocols and codecs specific to voice and video communications. The DMA provides a more secure, feature-rich and

robust implementation than the ALG feature of many firewalls. Firewall ALGs that have been implemented incorrectly can interfere with voice and video communications and should be disabled.

DMA edge services

The following sections summarize the services that would typically be run on a DMA. Note that services can be configured to run with an internal-facing Network Interface Card (NIC) connected to the internal network and an external-facing NIC connected to the external DMZ. Configuring services to use a single NIC is typically not recommended due to security and bandwidth implications. The NICs can be configured on the DMA's network configuration page. The specific ports that must be opened on the firewall and routed to the DMA depend on the services that run on the DMA and their specific configurations. See the System Port Ranges page in the *RealPresence Distributed Media Application (DMA) System Security and Privacy Guide* to view the ports required by DMA.

SIP

By default, SIP requires ports 5060 for unencrypted call signaling and 5061 for encrypted call signaling. These are the standard SIP signaling ports (use of different ports is not typically necessary). Additionally, the public outbound SIP ports must be open for outbound TCP traffic. The default range for these ports on DMA is 13001-23000 but this range can be modified on the *Service Config > SIP Settings* page. Any port range that's used must be matched on the firewall. The public outbound SIP ports are necessary to support multiple simultaneous SIP calls. Selecting a smaller range will limit DMA to a lower number of simultaneous calls.

H.323

By default, H.323 signaling requires ports 1719 and 1720. Additionally, H.323 dynamic ports are used in the same way as the public outbound SIP ports. The default H.323 dynamic port range is 35001-40000 and can be modified on the *Service Config > H.323 Settings* page. Any port range that's used must be matched on the firewall. The H.323 dynamic ports are necessary to support multiple simultaneous H.323 calls. Selecting a smaller range will limit DMA to a lower number of simultaneous calls.

WebRTC

By default, WebRTC requires the use of port 8443.

TURN

TURN is used in conjunction with WebRTC to enable call routing across NATs. By default, TURN uses port 3478. The TURN relay port range (used for establishing communication between endpoints when calls are made) is 60002-65535 and can be modified on the *Service Config > TURN Settings* page. Any port range that's used must be matched on the firewall.

External peers

In conjunction with the supported services, a DMA can be configured to communicate with one or more external SIP peers, external H.323 gatekeepers and external H.323 SBCs. These devices are used for routing calls within the internal network and to other organizations or cloud services outside of the internal network. By default, they use the same ports as the SIP or H.323 signaling services but can be configured to use different ports (see the *Integrations* menu). If they use different ports, those ports must also be open on the firewall if the external devices are only reachable on a separate network segment.

VPN tunnel

In a typical configuration, the ports that a DMA uses must be open on the firewall. In a VPN tunnel configuration, two DMA systems, one outside the firewall and one inside, can tunnel messages across the firewall through a single open port. This solution requires both DMAs to be actively involved in sending all video traffic as well as tunneling communication and encryption processing. Hence, this solution is resource intensive and DMA will have reduced system capacities.

An important thing to consider is that a VPN tunnel connects the public internet with a private local network. Another solution is to use two DMAs, one inside and one outside the intranet, peered to each

other, as shown in *Figure 1 in Sample Network Configurations* section of this paper.

Access Control Lists

DMA provides the ability to configure Access Control Lists (ACLs) for monitoring incoming traffic (H.323 and SIP). Based on the configured criteria of ACLs, the DMA either forwards traffic to the destination endpoints, or blocks traffic believed to be nefarious in nature. ACLs are meant to be specific to SIP and H.323 signaling and allow for dynamic determination of blocking. This can be as simple as blocking known attackers (the default ACL configuration), or more complex, such as blocking certain IP addresses, or allowing only provisioned endpoints to connect to the DMA system.

Security and redundancy

The DMA can be configured to support different levels of security to match the needs of an organization (*Admin > Security Settings* page). DMA runs on a hardened Linux OS and is designed to operate securely and redundantly. A pair of DMAs can be configured for High Availability (HA) so that one DMA can take over if the other fails.

DMA is also designed to use multiple network interfaces. This allows different services to run on different networks. For example, management traffic can be limited to the internal network to prevent possible intrusion from outside the local network. Devices that can access the management interface of the DMA can also be whitelisted.

DMA Deployment Wizard

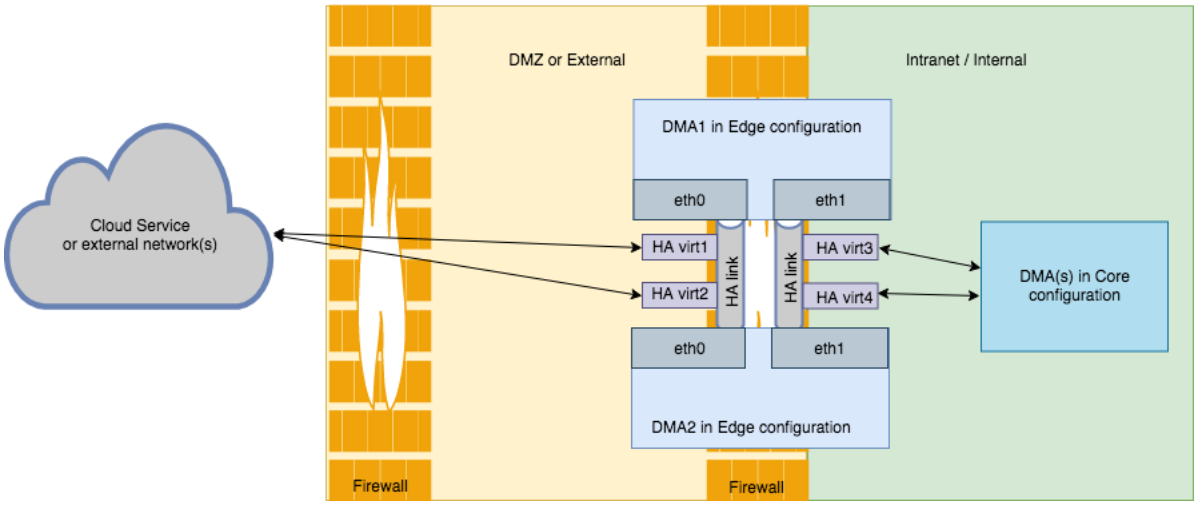
For ease of configuration of RealPresence DMA edge or combination server, DMA Deployment Wizard is available at https://dma-config.plcm.vc/. Once the DMA edge or combination servers are installed, the administrator can use the DMA Deployment Wizard to produce a backup file that can be restored on the DMA. The DMA Deployment Wizard is capable of generating the most common network and services configurations. Other configurations are simple modifications that can be done from the DMA web interface.

Sample Network Configurations

DMA supports a variety of network setups. The following examples describe several typical configurations.

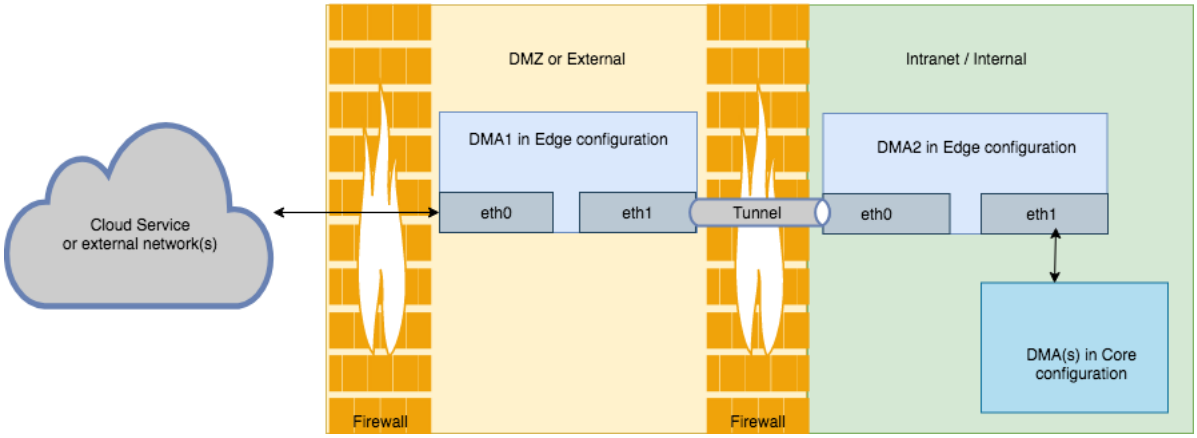
A recommended configuration option is for a DMA in edge configuration (or a pair of DMAs in edge configuration, configured for HA) to straddle the organization's firewall, as shown in ***Error! Reference source not found.***. No special ports between the intranet and DMZ need to be open since the DMA has NICs on both networks. The internal network, including a DMA in core configuration and any internal endpoints, MCUs, and other equipment, can safely communicate directly with the DMA in edge configuration. The DMA edge can use its external-facing NICs to communicate with the outside world, including any cloud services and external endpoints.

Figure 1: HA Pair of DMAs spanning the firewall



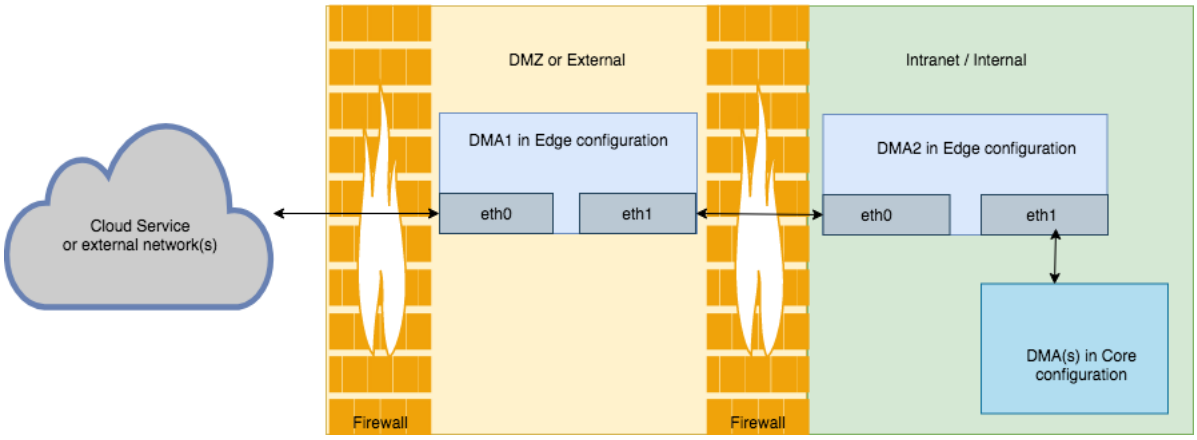
A second option is to set up a VPN tunnel between two DMAs in edge configuration, as shown in *Figure 2*. The advantage of this setup is that only a single port needs to be open for the VPN tunnel. The DMA edge in the DMZ can connect with any external networks, including cloud services and external endpoints. The DMA edge on the intranet can connect with all internal components. The two DMAs in edge configuration communicate with each other through the VPN tunnel, which requires a single port to be open on the firewall between them.

Figure 2: VPN tunnel between two DMAs



A third option is to peer two DMAs to each other using the External Peer feature, rather than establish a VPN tunnel (see *Figure 3*). This option will have better performance because the DMAs don't need to send all data through the VPN tunnel. In this setup, each DMA will share registration information with the other DMA. Unlike the VPN tunnel, ports on the firewall must be open for each service, instead of the single port used by the VPN tunnel. Note that this setup is only possible using DMA version 10.0 or later and cannot be used with RPAD systems.

Figure 3: Two DMAs peered across a firewall



Network Interface Configurations

A DMA typically has four network interfaces that can be used, eth0 – eth3 (other options, including VLANs and bonded interfaces, are outside the scope of this document). Different services can run on different network interfaces, and services which are aware of a public and private side can be further divided to run on two interfaces (for example, the signaling service can run on one network interface, or can be split between one public interface and one private interface). For DMA High Availability (HA) configuration, virtual IP addresses (that correspond to the subnet of the physical interface) are required for all interfaces that have services assigned to

them. If DMA is in an active/active HA configuration, two virtual IP addresses are required per interface with assigned services that correspond to the subnet of the physical interface. If DMA is in an active/passive HA configuration, only one virtual IP address is required per interface with assigned services that correspond to the subnet of the physical interface. Also, for HA configuration, the interface for HA Traffic Link will need to be specified. A second HA link is recommended for extra redundancy if multiple switches exist between the two servers.

The following tables show recommended network configurations:

Table 1: Configuration A – Separating signaling and media services on both public and private interfaces for maximum throughput

Number of NICs	Name of Interface	Assigned Traffic	Virtual IP for HA systems	HA Traffic Link for HA systems	Comments
4	eth0	• Management Services • Private (LAN) Signaling Services • Private (LAN) Access Proxy Services	Yes	Yes	
	eth1	• Private (LAN) Media Traversal Services	Yes	Yes	Optional second HA Traffic Link for extra redundancy
	eth2	• Public (WAN) Media Traversal Services • Public and Private TURN Services	Yes		Optional Public WAN-side and Private LAN-side TURN used for WebRTC calls
	eth3	• Public (WAN) Signaling Services • Public (WAN) Access Proxy Services	Yes		

Note: This configuration can be generated from the DMA Deployment Wizard.

Table 2: Configuration B – Separating management services and TURN services (optional) with its own interface respectively

Number of NICs	Name of Interface	Assigned Traffic	Virtual IP for HA systems	HA Traffic Link for HA systems	Comments
4	eth0	• Management Services	Yes	Yes	

	eth1	• Private (LAN) Signaling Services • Private (LAN) Access Proxy Services • Private (LAN) Media Traversal Services	Yes	Yes	Optional second HA Traffic Link for extra redundancy
	eth2	• Public (WAN) Signaling Services • Public (WAN) Access Proxy Services • Public (WAN) Media Traversal Services	Yes		
	eth3	• Public (WAN) TURN Services • Private (LAN) TURN Services	Yes		Optional Public WAN-side and Private LAN-side TURN used for WebRTC calls

Table 3: Configuration C – Separating private side management, signaling and media services from public side signaling and media services as well as optional TURN services on its own interface

Number of NICs	Name of Interface	Assigned Traffic	Virtual IP for HA systems	HA Traffic Link for HA systems	Comments
3 or 4	eth0	• Management Services • Private (LAN) Signaling Services • Private (LAN) Access Proxy Services • Private (LAN) Media Traversal Services	Yes	Yes	
	eth1	• Public (WAN) Signaling Services • Public (WAN) Access Proxy Services • Public (WAN) Media Traversal Services	Yes		
	eth2	• Public (WAN) TURN Services • Private (LAN) TURN Services	Yes		Optional Public WAN-side and Private LAN-side TURN used for WebRTC calls
	eth3	• No services assigned		Yes	Optional second HA Traffic Link (Direct Link) for extra redundancy

Note: This configuration can be generated from the DMA Deployment Wizard.

Table 4: Configuration D – Minimum number of interfaces configuration – with private management, signaling and media separated from public signaling and media

Number of NICs	Name of Interface	Assigned Traffic	Virtual IP for HA systems	HA Traffic Link for HA systems	Comments
2 or 3	eth0	• Management Services • Private (LAN) Signaling Services • Private (LAN) Access Proxy Services • Private (LAN) Media Traversal Services	Yes	Yes	Private LAN-side signaling and media TURN network services should be assigned to this interface, but the TURN server shall not be utilized in this configuration.
	eth1	• Public (WAN) Signaling Services • Public (WAN) Access Proxy Services • Public (WAN) Media Traversal Services	Yes		Public WAN-side signaling and media
	eth2	• Public (WAN) Media Traversal Services • Public and Private TURN Services		Yes	Optional second HA Traffic Link (Direct Link) for extra redundancy

Note: This configuration can be generated from the DMA Deployment Wizard.

Summary

A DMA in edge configuration serves as a solution for NAT and firewall traversal, allowing connectivity between an organization's internal video solution and the external internet.

At a minimum, some firewall ports need to be open and pointed to the DMA, as described previously in this document. DMA will route calls appropriately through networks, while also securing call traffic against potential attacks. In this respect, DMA acts in coordination with the organization's firewall and NAT to ensure connectivity and security.

For further details about more complex and customized configurations, refer to the *Polycom RealPresence DMA System Operations Guide* for your version of DMA.

To learn more about Polycom RealPresence DMA Service, please visit our product website.

Disclaimer

This white paper is provided for informational purposes only and does not convey any legal rights to any intellectual property in any Poly product. You may copy and use this paper for your internal reference purposes only. POLY MAKES NO WARRANTIES, EXPRESS OR IMPLIED OR STATUTORY AS TO THE INFORMATION IN THIS WHITE PAPER. THIS WHITE PAPER IS PROVIDED "AS IS" AND MAY BE UPDATED BY POLY FROM TIME TO TIME. To review the most current version of this white paper, please visit our website.

Additional Resources