A POLYCOM WHITEPAPER

Polycom® Recommended Best Security Practices for Unified Communications

October 2015

Unified Communications (UC) can be viewed as another set of data and protocols utilizing IP networks. From a security perspective, it is very similar to other IP data services, and Best Practices include technologies and methods used to protect other services. This document describes the security issues that organizations should consider as they deploy UC, and offers Polycom's recommendations for implementing secured UC.

Firewall Considerations

Polycom® Unified Communications devices are computing devices, and as such have remote management capability (through web GUI or other API). Like any IT asset, they should not be deployed outside the organization's corporate firewall without having these interfaces disabled. Polycom's recommended security best practice is to deploy these systems behind the firewall – as you would deploy any other high value IT asset – and use the Polycom® RealPresence® Access Director™ (RPAD®) or Video Border Proxy™ (VBP®) to enable firewall traversal of H.323 signaling and media streams. This helps ensure that attackers on the Internet are not able to randomly connect to unprotected UC endpoints.

Security benefit: Internet-based attackers are not able to reach open ports and services on UC devices deployed behind the firewall. Outside users, customers and business partners will still be able to make video calls to the UC device.

Other considerations: Organizations will need to deploy a UC Firewall Traversal solution such as the Polycom® RealPresence® Access Director™ (RPAD®) or Video Border Proxy™ (VBP®).

Note: Organizations that cannot use a firewall to protect video endpoints for cost reasons should disable remote management through the Security -> Enable Remote Management configuration menu, ensuring that Web, Telnet, and SNMP are not selected.

Firewall Traversal

The Polycom RPAD® or VBP® device provides Firewall Traversal for H.323 IP video. Working in conjunction with the organization's existing firewall, this allows for readily available video services without exposing the UC infrastructure or the rest of the organization's computers to attack. The RPAD® or VBP® can be used for both video access from remote users or for Business-to-Business video calls as shown below in figure 1.

Security benefit: The corporate firewall provides protection for UC devices just like it does for other IT assets. Outside users, customers and business partners are still be able to make video calls to the UC device.

Other considerations: Organizations should examine any Network Address Translation (NAT) architecture that they have in place, and may need to adjust to accommodate the firewall traversal.

Security Assessment Considerations

Polycom recommends that organizations periodically scan UC devices with vulnerability scanners and ensure that configurations mitigate any identified risks, just as you would for any IT asset. This is particularly important when deploying new UC devices to make sure that default configurations and passwords have not been left in place. Organizations should scan from both outside the firewall and inside the firewall for a complete view of the threat scenarios to outside attackers or to internal misuse.

Note that Polycom performs vulnerability scanning in its product

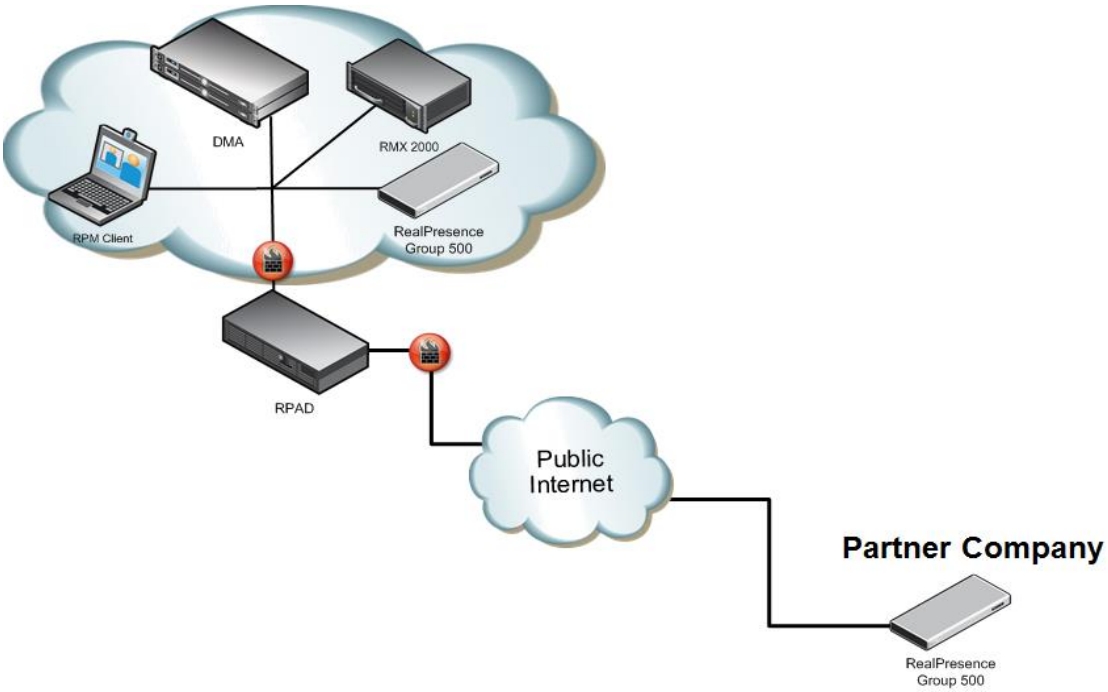

Figure 1: Business to Business Calling Example

release process.

Security benefit: Vulnerability scanning alerts the organization to missing patches or, more importantly for most UC deployments any security misconfigurations. Many commercial and Open Source scanners are available, including Internet-based scanning services. Scanning from outside the organization's firewall reveals weaknesses that an attacker could exploit from the Internet.

Other considerations: Scanning should be performed periodically to help ensure that configurations have not been changed. Scanning triggers alerts from Firewalls and intrusion Detection Systems (IDS). Note that Polycom does not recommend any particular scanning tool, and organizations should do their own investigation to select one appropriate for their needs.

System Management

IT administrators should treat UC video devices as typical computing devices for the purposes of administration. From a security perspective, administrators should take the same steps with these devices as they would with servers.

Unnecessary communications services should be disabled. If the organization is not planning to use Simple Network Management Protocol (SNMP) to monitor the devices, SNMP should be turned off. If the organization does not use the Polycom RealPresence® Resource Manager™ (RPRM®) management device, Telnet should be disabled. If SNMP is used for monitoring, organizations should change the SNMP default Community String ("public").

HTTPS should be enabled on all management interfaces so that system administration is done over secure connections where TLS/SSL is used to protect the transmission of sensitive data and authentication information

Vulnerability scanners identify which services are open and reachable. Unused services should be disabled.

Security benefit: The fewer services that are enabled, the fewer potential attack points an attacker could exploit.

Other considerations: Organizations should periodically examine system configurations to detect any changes that may have been made. Vulnerability scanners automate this process, and are recommended for periodic (monthly) checks.

Auto Answer Considerations

Auto Answer is the ability of the videoconferencing endpoint to automatically answer incoming calls. This feature is provided to make the system very easy to use, but the security implications of using this should be understood by organizations making use of it.

Why this is important: Many organizations find the convenience of Auto Answer to be critically important in how they use video. For example, a university might have a distance learning program where an instructor gives scheduled lectures from a particular classroom. These organizations will typically have remote classrooms automatically join the conference at scheduled times, and these remote classrooms depend on Auto Answer for this to work. From a threat perspective, the risk to the organization is relatively low, particularly if random Internet attackers cannot dial these classrooms.

Polycom recognizes that there is a balance that some organizations must strike between security and operations, and so recommends two different best practice configurations. Organizations need to consider their own risk tolerance in selecting one of these.

Most secure option: Disable auto answer.

Security risk: Risk is minimized for remote, unattended connections. If Auto Answer is not enabled, it is simply not possible for someone to dial into a room without the active cooperation of a user in that room.

Other considerations: This will not impact scheduled calls (Outlook integration, Polycom RMX, etc.), but it will require a user to use the remote control or the Polycom® Touch Control or other control system to answer the incoming call (i.e. just like a telephone). Note that if no one answers in 30 seconds, the call fails.

More open option: Auto answer is enabled (no action by user to answer incoming call).

Security risk: Remote, unattended connections can be made to video devices. Mitigations include:

1. Ensure that "Mute Auto Answer Calls" is set. Polycom® RealPresence® Resource Manager™ (RPRM®) can push this configuration out.
2. Disable far end camera control (Polycom RPRM® can push this configuration out).
3. Use a camera lens cover when the system is not in use.
4. RPRM® and the Polycom® Distributed Media Application™ (DMA™) Gatekeepers restrict calls to only those devices that are registered by the Gatekeeper. This essentially forms a closed community where auto answer is enabled but only viable from a known set of endpoints. (See DMA Operations Guide on Call Server Settings.)
5. Monitor Call Data Record (CDR) logs to make sure that calls do not come in at unexpected/unscheduled times.

Other considerations: It is important to ensure that the remote control is available and users understand that they have to unmute the call if this option is used.

Meeting Room Considerations

Auto Answer reflects a "Dial-in" use paradigm: outside participants dial in to a room video system. Polycom UC devices also support a "Dial-out" use paradigm, where video devices call a meeting room on a central video Multipoint Control Unit (MCU). This is an inherently more secure architecture than Dial-in, as there is no direct endpoint to endpoint connection – if a video room system has not connected to the MCU, a remote attacker simply cannot access that room, even if he can get access to the MCU.

Polycom extends this even further with DMA virtual meeting rooms. This not only shares the load across all available MCUs but makes it even harder for an attacker to guess where a particular video conference may be taking place.

Note that scheduled conferences can provide a "Dial-In" capability even when using MCUs or meeting rooms – the MCU will automatically call the video endpoints at the scheduled time, combining high levels of security with the highest ease of use.

Security risk: This configuration requires a video conference MCU such as the Polycom RMX. It would need to be deployed according to the recommendations in this document.

Other considerations: If this option is used, endpoints should not be configured with mute on answer.

Remote Access Considerations

Many organizations deploy video endpoints remotely, in Small Office/Home Office (SOHO) situations. These devices should be protected in the same way as any other remote IT asset. Virtual Private Network (VPN) technology is perhaps the most secure and most easily managed way to do this. Many vendors offer low cost, centrally managed VPN devices that can be deployed at these remote SOHO locations to protect the video device. Many of these (such as the Aruba RAP) include built-in firewall capability as well.

Security risk: The VPN makes the video device appear to be logically on the corporate network, protected by the corporate firewall. Internet users cannot access it, other than using normal video Firewall Traversal as they would for any video system. Because the video device appears to be on the corporate network, it is managed exactly as all corporate video devices.

Other considerations: Note that some home routers (for example, 2Wire) have trouble with NAT and Firewall Traversal. A remote VPN device avoids this issue.

Authentication and User Access Control

Polycom UC devices are computing devices, and while they are not general purpose computers like servers or desktops, they share much of the same security architecture. User accounts and passwords are one example of this.

Each Polycom device comes with an out-of-the-box default password. This should be changed on installation, as you would with any other computing device. The password should not be blank, should be a reasonable length, and should be changed periodically. Polycom UC devices enforce these aspects of good password policy.

Some organizations prefer to use Microsoft's Active Directory to manage user accounts and passwords, and Polycom devices support this configuration.

Security risk: Even the strongest device can be easily penetrated if it has a weak or default passwords. Organizations should assume that lists of default passwords are easily available on the Internet.

Other considerations: None.

Log Analysis

Polycom UC devices maintain a log of all calls placed and received. This log is called the Call Data Record (CDR), and organizations should regularly scan this log to see if the UC system is being used unexpectedly – to unexpected or unknown remote devices, at unexpected or unusual times like late at night, or when the room that contains the device was not scheduled or occupied.

The Polycom RPRM® management appliance can pull these CDR logs from all managed device for analysis.

Security risk: None.

Other considerations: Log analysis needs to be recognized as a formal IT task.

Toll Fraud

Organized and sophisticated groups of attackers continually scan the internet for systems that have not been secured against toll fraud. Lessening the threat of toll fraud attacks against VoIP and UC networks requires the implementation of safeguards and continuous monitoring. The RPAD® and VBP® include rules that can be enabled and fine-tuned for your environment that can block unwanted connections. If you don't have external extensions you should block unsolicited registration attempts at the firewall. Dial rules can be added to block known toll numbers or country codes that are not needed. Guest dialing can be disabled to block calls originating from un-provisioned or un-registered endpoints. The UC environment can also be configured to require endpoints to be registered so as to block un-registered devices from making connections. Use the encryption features included to protect data from eavesdropping and from allowing an attacker to steal credentials.

The UC infrastructure is just like the rest of the network and should be protected by layered defenses where the firewalls, IPS, IDS and

reporting all work together to protect the environment and alert administrators when something is happening that is not right.

Organizations should also conduct regular assessments of the UC environment including dial plans, firewall and routing rules and device configuration settings to ensure compliance with organizational policies are maintained.

Security risk: None.

Other considerations: None

Encryption

The biggest risk to UC communications is not from eavesdropping, but from attackers gaining access to the UC devices themselves. However, eavesdropping is possible, and tools are available to make this automated. Encrypting video communications helps eliminate this threat.

UC devices should be configured to use encryption when available. This will help ensure that older or third party devices that do not support encryption can still participate in UC conferences. Organizations that require higher security (or who do not have legacy systems to support) can configure UC devices to always use encryption.

Note that Polycom's encryption is FIPS-140, certified by the United States government.

Security risk: None.

Other considerations: Organizations requiring encryption at all times are not able to communicate with older devices (or third party devices) that cannot perform encryption.

Policy and Compliance Considerations

Polycom UC systems are designed to ensure that appropriate security requirements and security controls are implemented in such a way that they can be configured to meet a wide verity of information security policy and compliance requirements. These security controls and requirements are outlined in the Polycom Product Security Standards, a document whose controls are derived from and are developed to support widely accepted information security control standards such as NIST 800-53[1],ISO/IEC 27001[2], PCI-DSS[3] and COBIT[4]. As with any other IT system, your UC solution should be configured in such a way that it is compliant with your information security controls and policies. This will require planning, risk assessment as well as auditing and continuous monitoring.

Security risk: If UC systems are not configured to meet policy requirements, they may not align with compliance and audit requirements and may expose the organization to additional risks.

Other considerations: Review existing policies and compliance requirements as they may not include provisions for UC devices and may need to be updated.

Mobility Considerations

As video conferencing moves from static systems (such as room conference systems) to mobile devices such as laptop or table computers, organizations face additional security issues. While the video software is designed to work securely (for example, using encryption, etc.), the device itself is exposed to risks that static systems do not face, simply because it is mobile and outside of corporate protections.

Polycom recommends central management of mobile system video applications to help ensure that security configurations are properly set. The Polycom RPRM® management appliance provides this capability.

Polycom also recommends that 3rd party security software like antivirus, personal firewall, and configuration assurance are installed on the mobile devices. In addition, organizations should have a strategy in place to help ensure automatic updates to the mobile device OS and applications and for performing a remote wipe of sensitive data if the device is lost or stolen.

Security risk: Without central management of both video configuration and endpoint security, there is no way to predict if a mobile device might be used as a staging point for an attack on the organization.

Other considerations: Most antivirus vendors offer a client for mobile devices, and these integrate with the organization's existing antivirus console.

Business to Business Best Practices

Video calls that are between different business organizations pose special security risks, since each organization may have different security policies and controls. Unlike calls between members of the same organization, calls between organizations should be addressed by controlling the data flow to only devices of interest.

Most secure option: Use a Meeting Room.

Security risk: Risk is minimized by eliminating direct, point-to-point business to business calling. Both organization's endpoints call a video MCU deployed in the unsecured network area (DMZ). These MCUs are specially hardened for this type of deployment, and will link the endpoints into the same call. Note that the MCU should be configured in accordance of the recommendations in this document.

Other considerations: It is possible for the MCU to dial both endpoints at the time when the conference is scheduled to start. However, the remote organization should ensure that their endpoint is configured to allow this to be done securely.

More open option: Use Access Control Lists to restrict incoming calls. It is strongly recommended that frequent log analysis be performed to see if unexpected incoming or outgoing calls are being made.

Security risk: Remote connections can be made to video devices. Auto Answer mitigations should be implemented.

Other considerations: Firewall rules to allow incoming connections from the remote endpoint need to be configured in the firewall.

Device Disposal/Data Sanitization Considerations

When computing devices reach the end of their useful life and are disposed of, sensitive corporate data should be scrubbed from the devices. Polycom Unified Communications devices have the ability to do a Factory Reset, which restores the configuration to the initial, out-of-box configuration. This wipes all sensitive data (address book, call history, CDR logs, etc.).

Polycom recommends performing a factory reset on all UC devices prior to disposal.

Note: it is important to use the "Erase Flash" option when resetting the device to delete private data. This is described in the Polycom document HDX Volatility Statement.

[1] NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations,"

[2] ISO/IEC 27001:2013, "Information technology -- Security techniques -- Information security management systems – Requirements"

[3] PCI-DSS, "The Payment Card Industry Data Security Standard (PCI DSS)"

[4] COBIT, Control Objectives for Information and related Technology (COBIT)

About Polycom

Polycom is the global leader in standards-based unified communications (UC) solutions for telepresence, video, and voice powered by the Polycom® RealPresence® Platform. The RealPresence Platform interoperates with the broadest range of business, mobile, and social applications and devices. More than 400,000 organizations trust Polycom solutions to collaborate and meet face-to-face from any location for more productive and effective engagement with colleagues, partners, customers, specialists, and prospects. Polycom, together with its broad partner ecosystem, provides customers with the best TCO, scalability, and security for video collaboration, whether on-premises, hosted, or cloud-delivered. Visit www.polycom.com or connect with Polycom on Twitter, Facebook, and LinkedIn.

Polycom Worldwide Headquarters
6001 America Center Drive
San Jose, CA 95002
1.800.POLYCOM or +1.925.924.6000
www.polycom.com

4345_0312