Top 10 Reasons to Firewall Your Unified Communications Deployments

A common misconception is that firewalls and security appliances are incompatible with a unified communications solution. Firewalls, when correctly deployed, can provide an essential line of defense for unified communications. Here are the top 10 technical reasons to include firewalls in your unified communications proposals.

1. Phone Proxy: Campus Soft Phone Protection

Concerns about the security of end-user desktops have led some customers to defer deployment of soft phones in their unified communications systems. When a desktop is compromised, typically through exploitation of a data application, the attacker gains direct access to the communications manager cluster through the soft phone application. The Cisco® ASA 5500 Series Adaptive Security Appliance, with Cisco ASA Software Release 8.0.4, can be deployed as a phone proxy, which would force all soft phones to connect through the appliance rather than directly access the cluster. The appliance would then be able to apply a range of security services to protect the cluster from compromised soft phones.

2. Phone Proxy: Secure VLAN Traversal

Another customer concern is how to manage the security for calls between soft phones and hard phones. A standard design recommendation is to have hard phones separated from data devices and placed in their own phone VLAN. This works fine for hard phone deployments; however, because soft phones are applications that run on end-user desktops, they will reside within the data VLAN. When a soft phone calls a hard phone, the voice media needs to traverse from the data VLAN to the voice VLAN. With voice media communicating on a range of potential media ports, network administrators must open up numerous ports to ensure no disruption to service. This severely weakens the security of the VLAN separation. Using the Cisco ASA security appliance as a phone proxy helps ensure that the media always passes through a secure firewall proxy and that only legitimate voice media streams are allowed to traverse the VLAN boundary.

3. Firewall Access Control: Reconnaissance

Firewalls restrict access to networked servers such as Cisco Unified Communications Manager by filtering network traffic to only allow connectivity on the designated ports that the servers expect to communicate on. By preventing attackers from attempting to connect on rogue ports, the firewall can restrict the amount of information the attacker can gain, which is usually a precursor to more concerted attacks.

4. Firewall Access Control: Unauthorized/Illegal Access

Controlling access to User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) ports reduces the risk of an attacker exploiting a vulnerability in unified communications platforms and endpoints. At a minimum, implementing firewalls limits attackers to communicating to the infrastructure on the standard ports, preventing them from accessing potentially vulnerable nonstandard ports. To protect endpoints, unified-communications-aware firewalls are intelligent

enough to dynamically inspect the signaling traffic sent between the phones and the call control systems. The firewall dynamically opens up access to only the media ports that the endpoints determined during the signaling negotiation, keeping access to a minimum and helping to reduce risk. In contrast, standard access control lists (ACLs) have no such intelligence and must statically open up a wide range of UDP ports (16384 to 32767 for audio alone).

5. Intelligent NAT/PAT Services for Unified Communications Protocols

Although Network Address Translation (NAT) services are not recommended for unified communications deployments, there is sometimes a need to translate the network addresses of endpoints and the unified communications infrastructure. The challenge with applying address translation services to unified communications protocols is that signaling packets often include the network address both in the IP header and within the body of the packet. Traditional NAT and Port Address Translation (PAT) devices only translate the IP header; this results in the receiving party determining that there is a mismatch between the address in the IP header and the address in the body of the unified communications packet. In most cases, the receiving party will assume this is a rogue packet and will drop the packet and the connection. Truly unified-communications-aware firewalls can often perform intelligent NAT and can translate both the IP and embedded addresses within a unified communications packet.

6. Protocol Conformance

The most common vulnerability associated with unified communications is the risk of application servers being exploited by attempts at protocol fuzzing, where the attacker sends malformed packets to the server with the expectation that the server will not be able to correctly process those packets. This can result in an interruption of service, the disabling of the server altogether, or, in extreme cases, enabling the attacker to remotely control the server itself. The Cisco ASA security appliance, Cisco Firewall Services Module, and Cisco IOS® Firewall are all capable of checking the conformance of the incoming packets to the standards for that protocol.

7. Application Inspection and Control: Registration Enforcement (SCCP Only)

Truly unified-communications-aware firewalls, such as the Cisco ASA, are able to apply specific unified communications policy to traffic that passes through them. For example, Cisco ASA security appliances can enforce device registration before any requests for unified communications services are made. Rogue devices that may seek to send unsolicited call requests to the Cisco Unified Communications Manager can be blocked by the appliance, which maintains a state table for all devices that have successfully registered. Devices that have not registered and that attempt to place calls can be automatically blocked and their information logged or recorded. This applies to Skinny Client Control Protocol (SCCP).

8. Application Inspection and Control: Block Rogue Callers

If customers experience problems with inbound calls from rogue callers, certain firewalls can implement application inspection and control features for unified communications and are able to filter out specific callers. The call invites [[invitations?]] can be blocked and the call attempts can be logged and recorded.

9. Rate Limiting: Denial of Service Prevention

Attackers may seek to create a denial of service condition by overwhelming the communications manager with an excessive number of call requests. Cisco ASA security appliances can be deployed to protect the call control cluster by rate limiting the number of Session Initiation Protocol (SIP) invitation messages that can be sent from a particular endpoint.

10. Media Inspection (RTP/RTSP): Media Insertion and Disruption

Attackers may seek to inject spurious media into legitimate media conversations. This can distort the audio or video media, resulting in unintelligible audio or potentially the insertion of audio from the attacker. Firewalls that support Real-Time Transport Protocol/Real-Time Streaming Protocol (RTP/RTSP) inspection are able to verify the media being sent between the two parties and can reduce the risk of media insertion and disruption.

Summary

As IP voice infrastructures evolve into true unified communications infrastructures, there is a stronger case for supplementing the existing security in the applications, endpoints, and call control with that available within network and security platforms. The increasing trend toward remote access and mobility services for unified communications adds additional security considerations to those already present within the campus and branch networks. Cisco adaptive security appliances, along with other—communications-aware Cisco firewalls, provide an essential first line of defense against a range of potential threats and risks.

For more information on Cisco Secure Unified Communications, visit http://www.cisco.com/go/secureuc

For more information on the Cisco ASA 5500 Series Adaptive Security Appliance platform, visit http://www.cisco.com/go/asa

For more information on the Cisco IOS Firewall Feature set for Cisco IOS Software-based routers, visit http://www.cisco.com/go/iosfw

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-492026-00 08/08