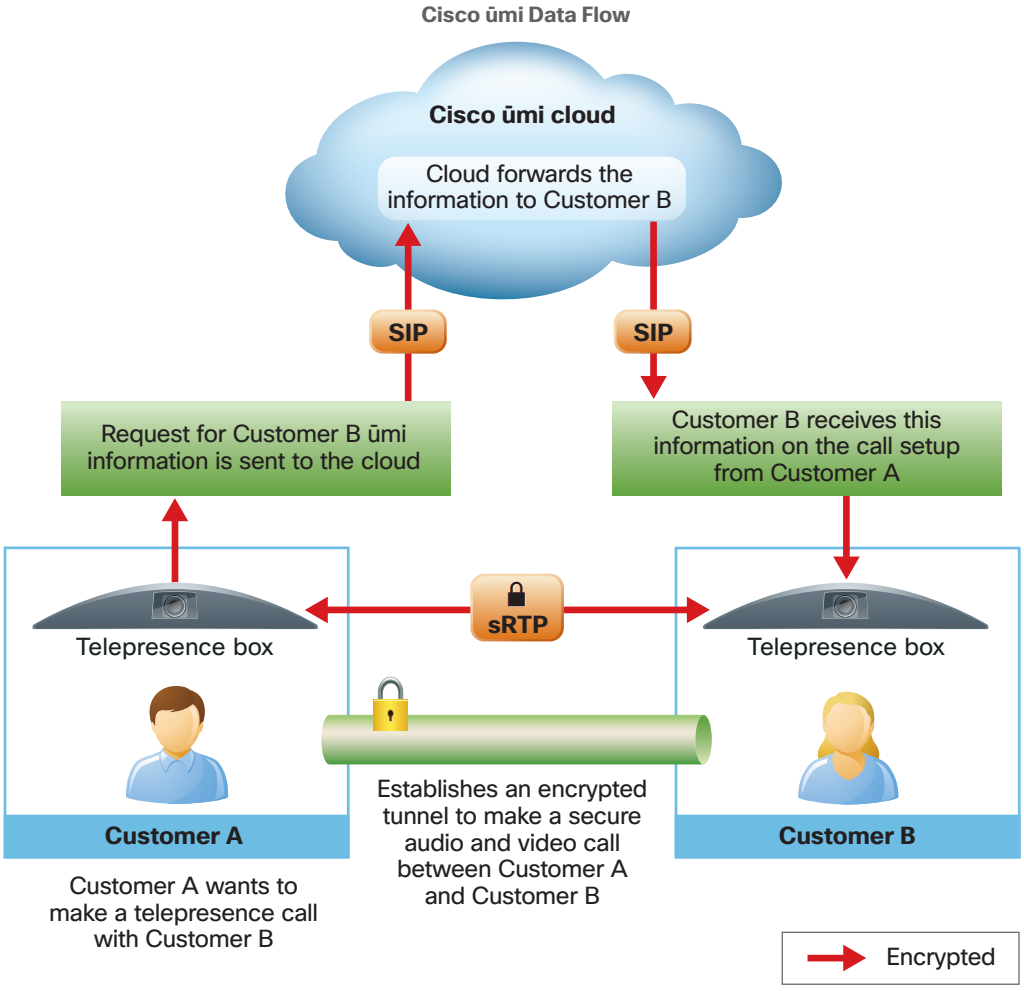
Keeping ūmi Communication Secure: A ūmi Security Whitepaper

Introduction

Cisco ūmi telepresence connects to a member's HDTV and broadband network to deliver a natural communications experience similar to what one would experience if he or she were in the same room with friends and family—even though they are thousands of miles away. Cisco ūmi transforms standard-definition video conferencing into high-definition telepresence, where the objective is not just to see or hear someone who is at a remote location, but to provide an experience so clear and lifelike that ūmi callers will see what each other sees, hear what they hear, and feel what they feel.

The following diagram depicts the flow of data in a ūmi call:

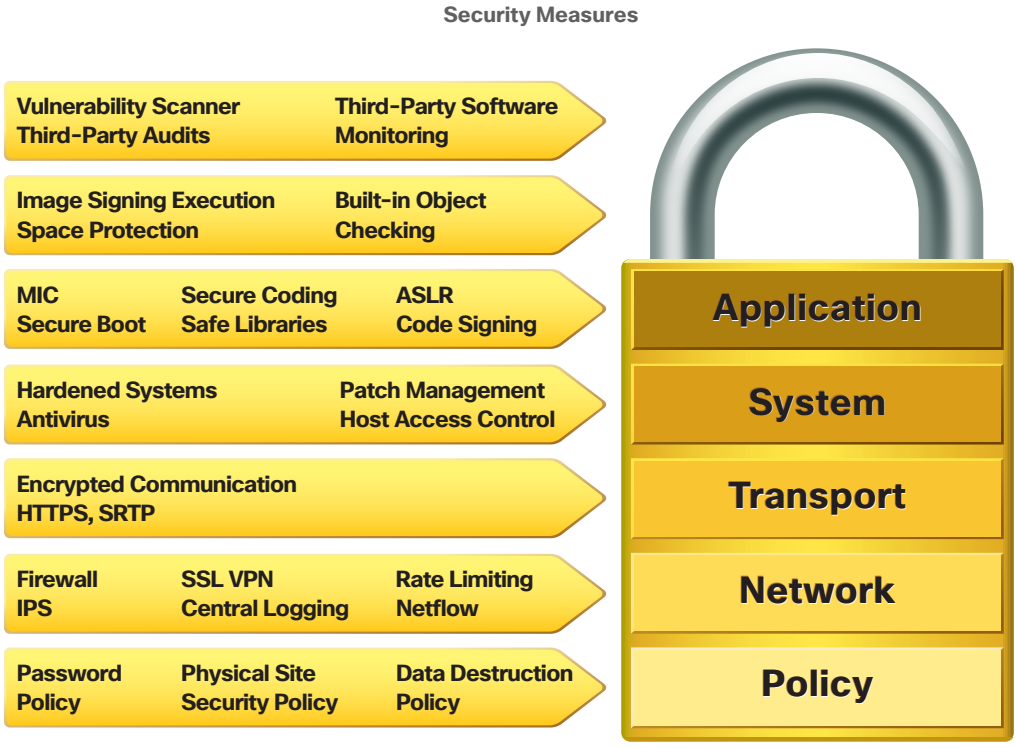


At the heart of ūmi traffic flow lies the Cisco ūmi cloud, which provides a highly available and secure service delivery platform, unburdened by the physical limitations of an on-premise solution. As shown in the diagram, the Cisco ūmi cloud contains multiple resources that are available to each member, including making a ūmi call and or retrieving a video message.

To ensure the integrity of communications through the Cisco ūmi cloud, the Cisco ūmi security team has implemented a number of layered security measures. This paper describes those measures, including those built in to the Cisco ūmi cloud architecture, those implemented on the ūmi console (endpoint), and others.

Cisco ūmi cloud architecture security features

The Cisco ūmi cloud has been architected not only with “scale” and “high availability” in mind, but also with various security defenses. The following diagram provides a schematic presentation of all components of the cloud security architecture. Select security measures are described in more detail in the sections that follow the diagram.



Host and network device hardening

The Cisco ūmi security team has developed specific hardening guidelines not only for the operating system, but also for the network and any applications that are deployed in the ūmi cloud. The hardening guidelines encompass all the leading security guidelines and are reviewed and updated on a regular basis as new attack vectors are identified.

On each console (endpoint), a compliance scan is performed on a regular basis to ensure that the defined guidelines are being followed.

Firewall

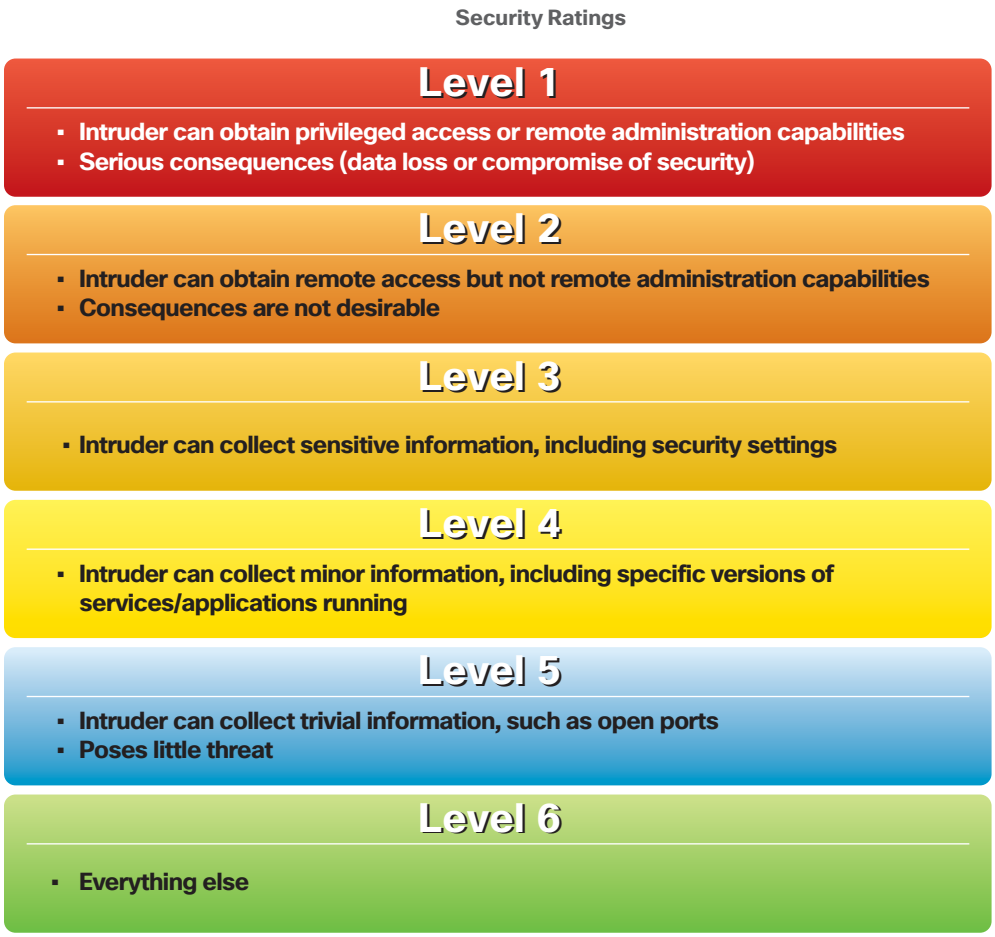
For all inbound and outbound Cisco ūmi traffic, the default configuration is to deny all traffic. Ports are opened to allow traffic through authorized ports and IP addresses only. The level of security afforded by the firewall is a function of which ports are opened by the customer, and for what duration and purpose. The Cisco ūmi cloud uses a traditional three-tier architecture, in which web servers, application servers, and database servers have designated ports available to designated groups. In this architecture, all external traffic is allowed to access only the web server group, which resides external to the cloud.

File integrity monitoring

All systems have file integrity monitoring enabled for critical system files, configuration files, content files, and log files that constitute required audit trails.

Patch management and third-party vulnerability notification

In the Cisco ūmi cloud, all packages and kernels are registered with the Cisco Security IntelliShield Alert Manager Service. This service keeps tracks of new threats and vulnerability alerts. Any time an update or security patch is released, the Cisco ūmi security team reviews the attack and extent of exposure, and applies the remediation in a timely manner. The speed of the response directly corresponds to the severity of the attack. The various attack severity levels are shown in the following diagram:



Vulnerability scanning

The Cisco ūmi security team performs both internal and external scans on the environment on a regular basis. This database is constantly updated. Any security issue detected is remediated in a timely manner based on the severity level, as shown in the preceding diagram.

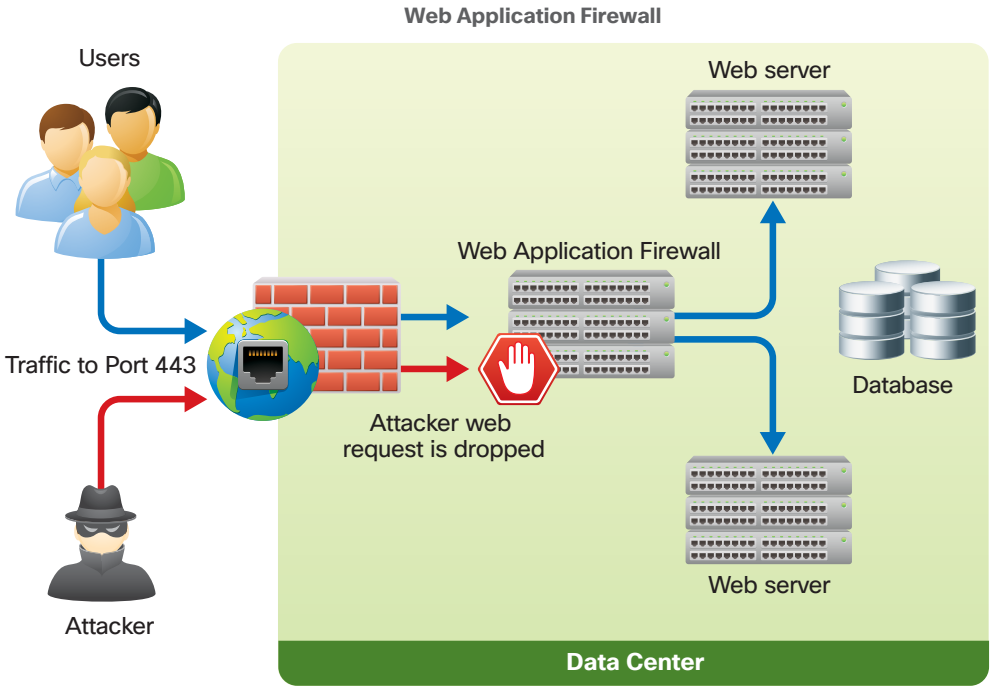
Intrusion prevention system

The Cisco ūmi security team monitors the environment using the industry's top-of-the-line Cisco Intrusion Prevention System. The Cisco ūmi security team works diligently to update the signature and correlation rules for all security attacks.

Web Application Firewall

The Web Application Firewall is an appliance that monitors all HTTP conversation. Each monitored conversation is matched to a set of custom rules, which check for web security issues such as cross-site scripting, SQL injection, web server failures, coding errors, and so on. The Web Application Firewall also provides a mechanism to write custom rules, identify attacks, and block attacks. All traffic classified as an attack is blocked by the Web Application Firewall.

The following figure shows a typical deployment of the Web Application Firewall appliance:



Central logging and correlation

The Cisco ūmi security team collects logs from all applications, networks, and systems. All these logs are indexed and correlated. Reports are then generated based on various security incidents. These incidents are reviewed on a regular basis.

Multiple levels of security audit

The Cisco ūmi cloud has gone through multiple third-party security audits, performed by industry leaders. Any security vulnerabilities were remediated to protect the cloud and prevent any security attacks.

Distributed denial of service (DDoS) attacks

The Cisco ūmi cloud is hosted and utilizes world-class Cisco devices. The cloud is designed with standard defenses for any DDoS attacks, which include limiting the number of connections allowed.

Security features on the ūmi console

sUDI (Secure Unique Device Identification)

The sUDI, also known as the Manufacturing Installed Certificate (MIC), is a type of X.509 certificate. The sUDI is used for authentication in the Cisco ūmi cloud and performs the following security functions:

- provide a mechanism for uniquely identifying each ūmi console (endpoint)
- establish a secure SSL VPN connection to the Cisco ūmi cloud
- encrypt the initial handshake for the traffic between two ūmi members.

Security considerations for data in motion

All traffic between a ūmi console and the ūmi cloud is transmitted using the secure HTTPS protocol. In addition, all data values identified as critical—such as password, credit card number, and so on—are first encrypted using AES 256 before being transmitted over HTTPS. This provides an additional layer of protection of user data.

NOTE: For more information on HTTPS, please visit **http://tools.ietf.org/html/rfc2818**.

The Cisco ūmi product also utilizes the following authentication methods:

- GSSAPI-based authentication
- Host-based authentication
- Public key authentication
- Challenge-response authentication
- Password authentication

Inside the Cisco ūmi cloud, communication between the servers is encrypted with the highest level of encryption.

Administration

Two-factor authentication is required to gain access to the Cisco ūmi cloud. All operations and activity in each console are logged, and a report of all activity is generated and reviewed weekly. Any insecure communication detected to or from the administration is disabled to prevent any possible exposure.

Compliance

The Cisco ūmi product adheres to all compliance requirements for a product of its type and class.