White Paper

Keeping Cisco OnPlus Service Communication Secure: A Cisco OnPlus Security White Paper

Introduction

Cisco OnPlus™ Service is a simple, affordable. cloud-based platform that enables reseller partners serving small businesses to deliver managed network services through discovery and monitoring of the entire small business network. Easy to deploy and use, it lets partners securely access customer networks from anywhere, at any time, using a variety of devices.

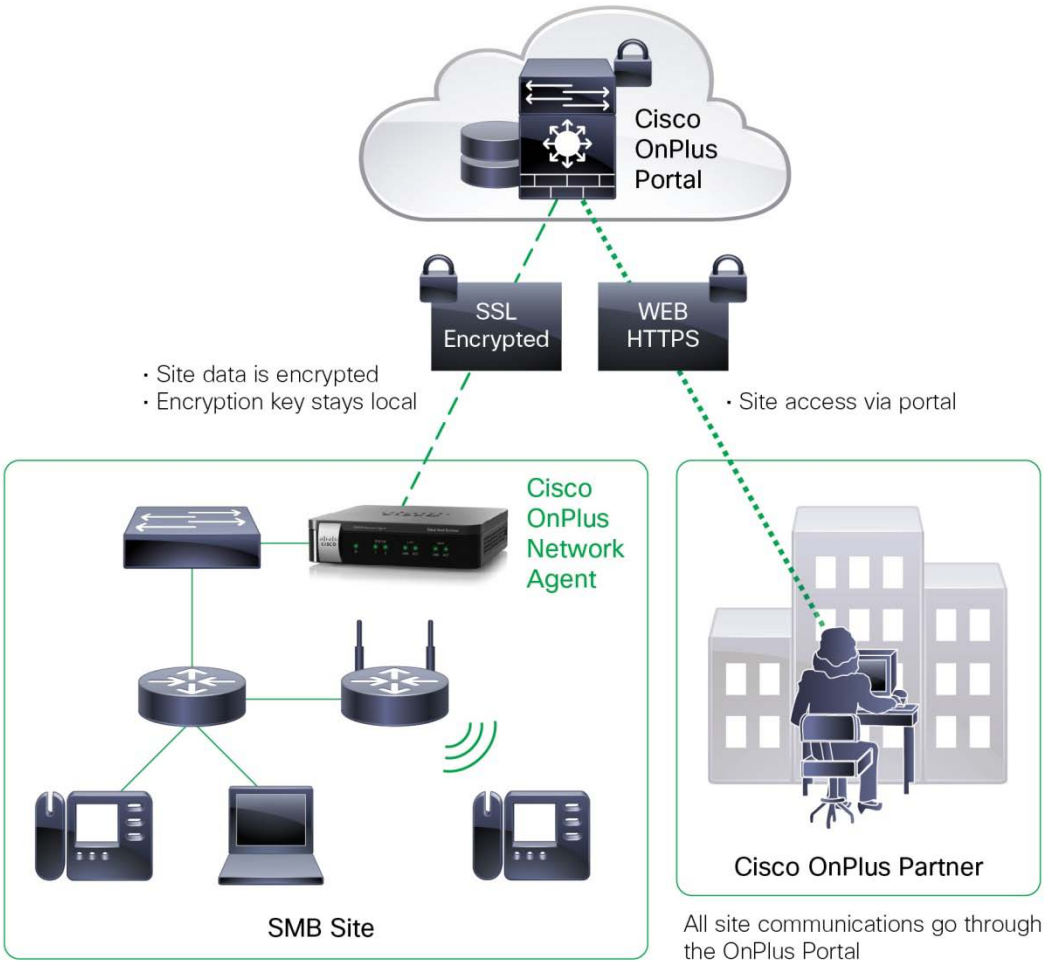
Cisco OnPlus uses an appliance, the Cisco OnPlus Network Agent, installed at the customer premises, to discover network devices and collect data on the network and to provide secure connectivity to those devices. Through a persistent connection to the Internet, the Cisco OnPlus Agent transmits this data to a secure data center.

Cisco OnPlus discovers Cisco® and third-party devices with an IP address on the network and displays them in topology and inventory views. Partners can access a view of customer networks from anywhere, at any time, through a highly secure portal using a PC, tablet, or mobile device. Reseller partners can define and customize alert thresholds to enable proactive support and device management. For Cisco devices, the service also supports configuration backup and restore, application of firmware updates, and warranty and support contract status. Finally, OnPlus provides automated, summarized reports of all the activity and tasks performed on the network.

To help ensure the integrity of communications through the Cisco OnPlus Service cloud, the Cisco OnPlus security team has implemented a number of layered security measures. This paper describes those measures, including those built into the Cisco OnPlus Service cloud architecture, those implemented on the Cisco OnPlus Network Agent, and others.

Figure 1 depicts the flow of communication among the Cisco OnPlus Service in the cloud, the partner's computer accessing the OnPlus Portal, and the partner's customer sites.

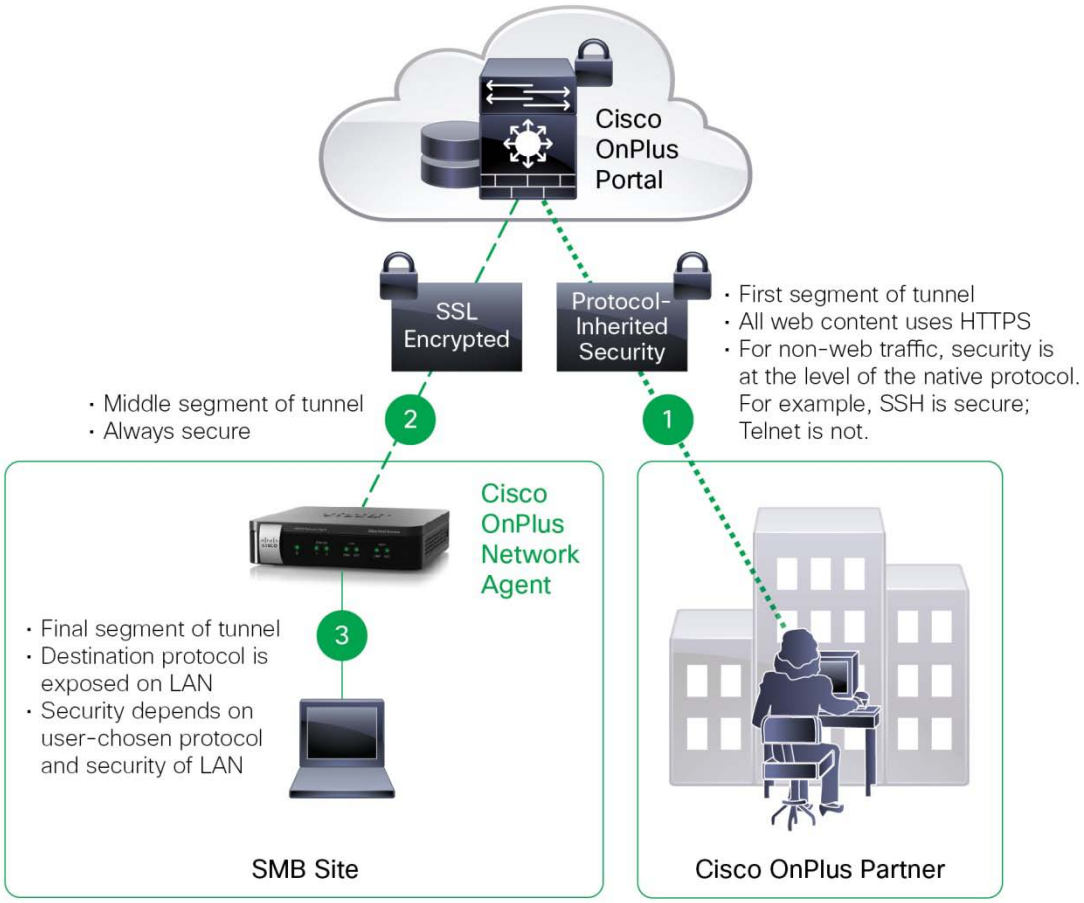
Figure 1. Cisco OnPlus Service Data and Communications Flow



Remote Connections via the OnPlus Portal

The remote connection feature allows one computer at a time outside the OnPlus Network Agent's site to communicate with a device on the customer network through the OnPlus Portal. The connection involves a single TCP port over one or more connections, using either web (HTTP/HTTPS) or non-web protocols. When using web protocols, a browser session cookie is used to help ensure that only the browser that created the tunnel can connect to the tunnel. Non-web-based protocols do not use cookies. For these protocols, the tunnel is locked to allow only packets from the original web browser's public IP address. Both the web-based and non-web-based tunnels automatically expire when the tunnel becomes idle, and the tunnel is removed after it expires. Partners can choose to disable this feature for a customer if needed.

Figure 2. Remote Connections to Customer Devices via the OnPlus Portal



The middle segment of the tunnel—between the Cisco OnPlus Portal and the OnPlus Network Agent—is always encrypted and secure.

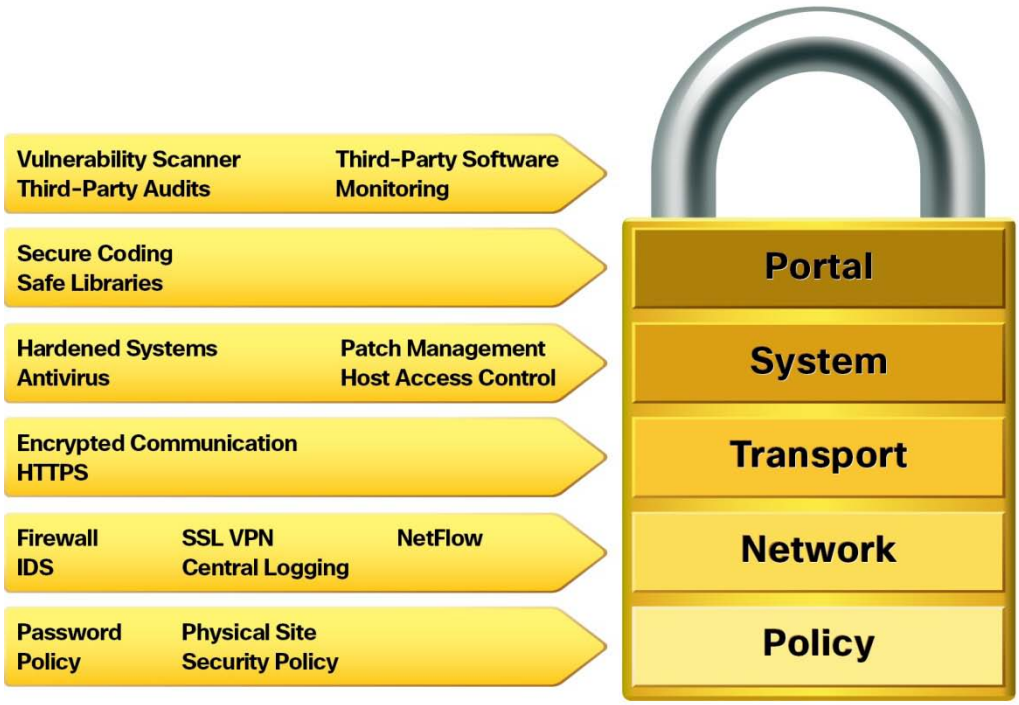
The first segment of the tunnel—between the partner's computer and the OnPlus Portal—is always encrypted for web traffic (HTTPS/HTTP). However, for non-web traffic between the partner's computer and the Portal, security depends on the protocol that the partner chooses to route traffic through the tunnel. For example, Secure Shell (SSH) is secure, but Telnet is not.

The final segment of the tunnel is between the OnPlus Network Agent and the tunnel's target device at the customer site. It is expected that either this last segment of the tunnel is on a subnet served by the same router as the OnPlus Network Agent or that the path to the target is encrypted (through a VPN). The security of the last segment also depends on the security of the partner's chosen protocol; security is improved when the target device and the OnPlus Network Agent are both on the same secure private network.

Cisco OnPlus Service Cloud Architecture and Security Features

The Cisco OnPlus Service cloud has been architected not only with scale and high availability in mind, but also with various security defenses. Figure 3 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.

Figure 3. OnPlus Cloud Security Architecture



Host and Network Device Hardening

The Cisco OnPlus 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 Cisco OnPlus 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 the OnPlus Service cloud host system and network, a compliance scan is performed on a regular basis to ensure that the defined guidelines are being followed.

Firewall

The OnPlus Service cloud default configuration is to deny all inbound traffic. Ports are opened to allow traffic through authorized ports only. The OnPlus cloud restricts all external traffic against direct access to internal facilities. Applications receiving direct external traffic operate with restricted privileges and access.

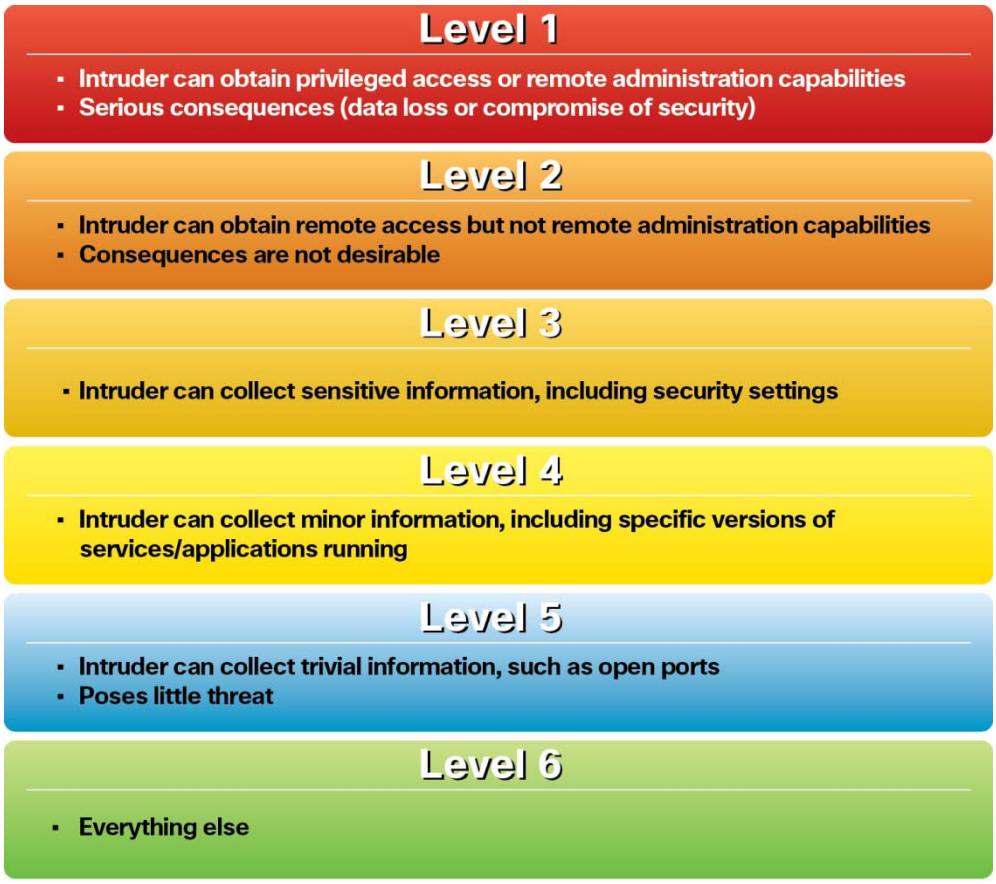
File Integrity Monitoring

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 Notifications

In the Cisco OnPlus cloud, all packages and kernels are registered with the Cisco Security IntelliShield Alert Manager Service. This service keeps track of new threats and vulnerability alerts. Any time an update or security patch is released, the Cisco OnPlus 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. Attack severity levels are shown in Figure 4.

Figure 4. Attack Severity Levels



Vulnerability Scanning

The Cisco OnPlus 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 manager, based on the severity level, as shown in Figure 4.

Intrusion Detection System

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

Web Application Security

The Cisco OnPlus Portal implements a number of security features. An Application Login Tarpit is used to defend against brute force attacks. Each failed login attempt exponentially slows the server's response to the attacker. To protect against session hijacking, the OnPlus Portal uses IP Source Locking. With IP Source Locking, each valid user session is tied to the originating source IP address. If a valid session ID is supplied by a client with a different IP address, the valid session is terminated.

To defend against SQL injection and cross-site scripting attacks, the OnPlus Portal uses Lowest Level Permissions. In a typical web application, all users have permission to view all data in the database. This requires the web application to enforce strict permissions to ensure that a user cannot access or modify another user's data. To protect against elevated privilege attacks, OnPlus Service application security and permissions are pushed to the lowest level possible: the database. The OnPlus Portal user does not have permission to view, modify, or remove any other user's data inside the database, even if the user gains console access to the database itself.

The OnPlus Portal also requires that all HTTP POST requests include a valid HTTP referrer. Typically, these originate from the user's web browser. Most add, modify, and delete operations inside the OnPlus Portal require an HTTP POST request, so this protects these portal operations from cross-site forgery request attacks.

Central Logging and Correlation

The Cisco OnPlus security team collects logs from all application, networks, and systems. All of 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 OnPlus 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 OnPlus cloud is hosted and uses world-class Cisco devices. The cloud is designed with standard defenses for any DDoS attacks, which include limiting the number of connections allowed.

Data Protection and Segregation

The Cisco OnPlus Portal uses database partitioning to help ensure that authenticated users and devices cannot accidentally see data that they are not entitled to access.

The Cisco OnPlus cloud requires a valid Cisco.com password for access. To limit any chance of exposure of that password, all internal access is based on a time-limited SHA256 digest of that password. This means that the password is never transmitted internally in the system (in clear text or encrypted) once the initial session login has been authenticated.

Device credentials entered on the OnPlus Portal by a partner for enhancing device discovery, enabling portal features, and support are encrypted using the specific OnPlus Network Agent's unique public encryption key, then stored in the portal database. The private key for the OnPlus Network Agent never leaves the OnPlus Network Agent at the customer site and is used only to decrypt secure content provided by the portal.

The OnPlus Network Agent's X.509 encryption/decryption key pair is generated when the OnPlus Network Agent is first powered on and any time it is restored to factory defaults. This ensures that the X.509 key pair is never reused when an OnPlus Network Agent is transferred from one customer site to another.

Security Features on the OnPlus Network Agent

The OnPlus Network Agent provides minimal external access due to the nature of its discovery technology and reliance on user interactions with the Cisco OnPlus Portal. The only user access to the OnPlus Network Agent is provided via a web-based interface using password authentication. The random password is automatically generated when the customer account is created, and the portal user can change this password as needed. The OnPlus Network Agent firmware is upgraded to safe versions as required using guidance from the Cisco Security IntelliShield Alert Manager Service. New firmware is delivered through the Cisco OnPlus Portal. If needed, firmware with security fixes can be delivered within 24 hours to all active sites, once a solution is committed.

Administration

All Cisco OnPlus operations and activity in the cloud are logged, and a report of all activity is generated and reviewed on a regular basis. Any insecure communication detected to or from the administration is disabled to prevent any possible exposure.

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 C11-690328-00 10/11