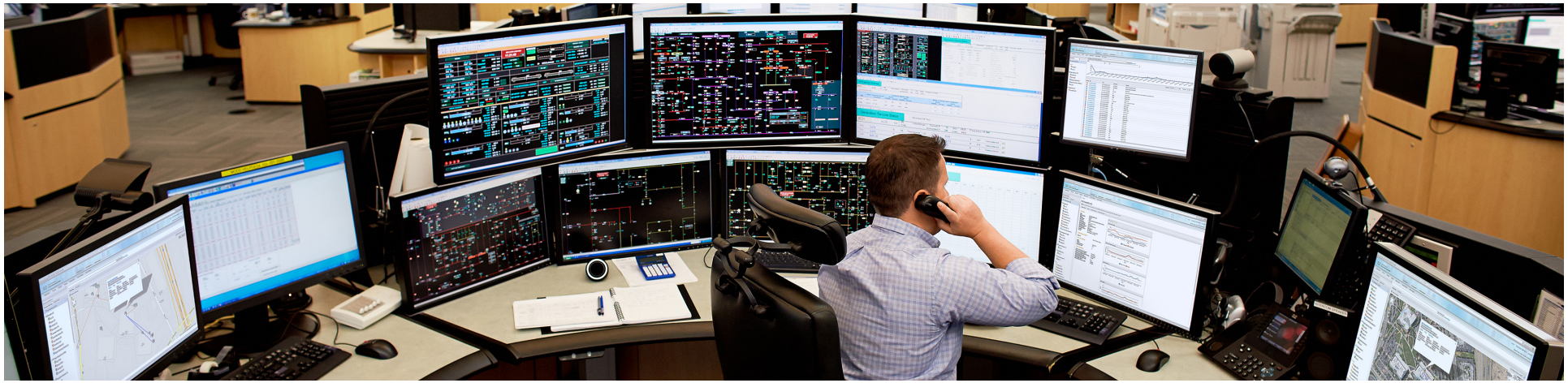
Use Case: Managed Mobility Security and VPN Service

GENERATE NEW REVENUE FOR MANAGED SERVICE



What Is the Value of the Managed Mobility Security and VPN Service?

Operators can provide enterprises with a Managed Mobility Security and VPN Service that provides highly secure VPN access for mobile devices over the service provider managed WAN. The service brings new revenue to operators while enabling customers to outsource management of the WAN so internal IT resources can be redirected to more strategic projects instead of network infrastructure management. The set monthly costs based on agreed upon SLAs support more accurate budgeting and allow customers to shift operational and capital expenditures from network support to other business-critical initiatives.

What Problems Does It Help Solve?

Reliable, encrypted mobile network connectivity and persistent corporate access for users on the go with smartphones, tablets, and other mobile devices is a service many enterprises may be interested in outsourcing because it is viewed as infrastructure management instead of a strategic, mission-critical IT initiative. Mobile operators can provide their infrastructure to deliver dependable, consistent access, whether users are checking their business email, launching a virtual desktop session, or utilizing other enterprise applications.

Based on the Cisco AnyConnect Secure Mobility Client and other Cisco and partner technologies, the Managed Mobility Security and VPN Service features an easy-to-use interface to business-critical information. For the operator, the client is easy to deploy and manage. Integrated security and device management products provide robust security features and real-time management of the mobile WAN environment. For the enterprise customer, secure mobile access is as easily outsourced as cellular service and the consistent monthly fee is a welcome departure from often unpredictable internal operational and capital expenditures.

What Are the Benefits of the Managed Mobility Security and VPN Service?

- Generate new revenue from managed service
- Upsell additional services as the customer's requirements evolve

What Do I Need?

The Managed Mobility Security and VPN Service requires intelligent network technologies that control policy, charging, and subscriber data management.

Cisco solutions to enable you to deliver the Managed Mobility Security and VPN Service along with many other revenue-generating services include:

Cisco Solution	Description
Cisco ASR 5500 Multimedia Core Platform	Part of the Cisco ASR 5000 Series packet core platform, the Cisco ASR 5500 Multimedia Core Platform combines massive performance and scale with flexibility, virtualization, and intelligence so network resources are available exactly when they are needed. The Cisco ASR 5000 Series' elastic architecture enables its software-based mobile functions to utilize system resources across the entire platform to optimize performance and maximize efficiency. This approach allows operators to deploy more efficient mobile networks that can scale to support a greater number of concurrent sessions, optimize resource usage, and deliver enhanced services. Integrated Deep Packet Inspection (DPI) and value-added services on the Cisco ASR 5000 Series are deployed within the data session instead of requiring it to be off-loaded to standalone platforms. Individual Wi-Fi subscriptions can be part of an overall mobile data plan and Wi-Fi traffic can be carried though the packet core to preserve the same service privileges and limits for the subscriber whether on Wi-Fi or mobile cellular networks. In version 1.0 of Cisco Access Network Discovery and Selection Function (ANDSF), service providers can create policies to offload subscriber devices to Wi-Fi when they are within range of the operator's hotspots, based on current values of certain attributes in the operator's subscriber database (including location, quality of service, time of day, prepaid versus postpaid, Gold/Silver/Bronze level, etc.). The ANDSF server can trigger Cisco Anyconnect VPN when the Wi-Fi network is marked as not being secure.
Cisco AnyConnect Secure Mobility Solution	Cisco AnyConnect Secure Mobility solution, powered by the industry's leading firewall, the Cisco ASA 5500 Series Adaptive Security Appliance, offers a comprehensive suite of VPN access features along with powerful security features. It allows administrators to provision remote access through appropriate security policies for a variety of endpoints – from Mac or Windows environments to the latest iPad, iPhone, and Android devices – using multiple access methods, such as the user-acclaimed Cisco AnyConnect® Secure Mobility Client or the Cisco clientless portal for any Web browser.
Cisco Identity Services Engine	The Cisco Identity Services Engine (ISE) is an all-in-one enterprise policy control product that enables comprehensive secure wired, wireless, and VPN access, leading to more productive workers and lower operations costs. When operating in a network, ISE provides an array of features, including rigorous identity and policy enforcement, security compliance, automated onboarding, automated device security, anywhere access, operational efficiency, embedded profiling enforcement, next-generation Cisco TrustSec® policy networking, an ecosystem of solution partners, and more.
Mobile Device Management	Cisco Meraki Mobile Device Management provides unified management of mobile devices, Macs, PCs, and the entire network from a centralized dashboard. Security policies can be enforced; software and applications can be deployed; and remote, live troubleshooting can be performed on thousands of managed devices. The integration of Cisco Meraki Mobile Device Management and Cisco ISE provides comprehensive and flexible network-wide policy-based controls for mobile devices, including Bring Your Own Device (BYOD) initiatives. With this integration, no rogue devices can connect to the network, additional information about endpoints that cannot be gathered by network-based profiling can be obtained, periodic compliance checks are conducted to ensure that the state of each mobile device is still in compliance with company policy, and IT administrators can trigger remote actions from the ISE administration interface such as lock or wipe device.

Why Cisco?

The Cisco Open Network Environment (ONE) converges physical hardware and virtual software technologies to make the network easier to program, access, use, operate, and manage. Cisco ONE can help you drive new revenues and monetize your network in new and profitable ways. Cisco's solutions, platforms, and technologies provide a scalable, standards-based intelligent IP architecture that enables you to integrate subscriber knowledge with network and application intelligence in real-time to offer an expanding portfolio of "Use Cases," which are innovative, revenue-generating applications and services that:

- Drive profitable data revenues by providing user personalization and seamless, secure heterogeneous access across 3G, LTE, and Wi-Fi networks
- Evolve your network into a platform for both direct and third-party partner monetization
- Enable you to establish profitable new business-to-business-to-consumer (B2B2C) revenue models
- Help you enter new, growing markets such as cloud services, content delivery, enterprise services, location-based services, machine-to-machine (M2M) applications, and more

To help deploy mobile Internet solutions efficiently and successfully, Cisco Services offers consulting for design, implementation, integration, and support.

For more information, please visit: http://www.cisco.com/go/mobile.

C45-731332-00 07/14