Miercom

Lab Testing Summary Report

October 2007
Report 071015

Product Category:
Remote Access

Vendor Tested:
Cisco Systems

Product Tested:
Enterprise Class Teleworker solution

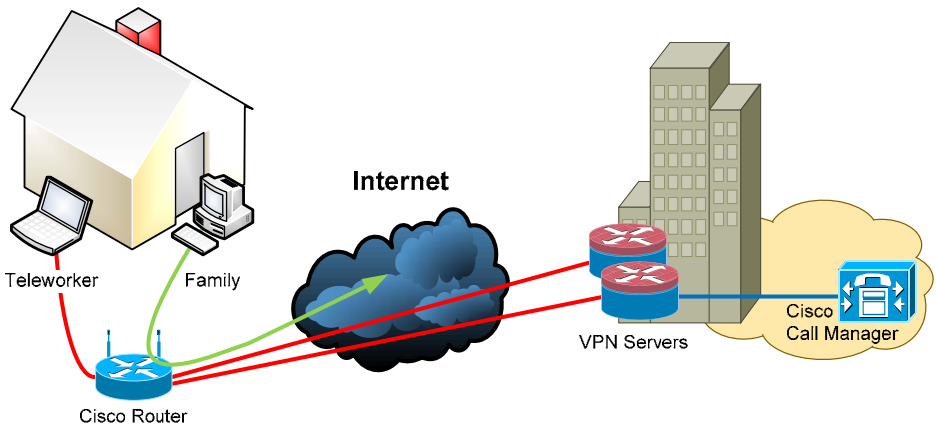
Key findings and conclusions:

- **Enterprise-class teleworker (ECT) solution enabled through Cisco Integrated Services Router platforms**
- **ECT enables voice, video and data solutions for enterprise teleworkers**
- **Zero-touch deployment improves manageability and service roll out**
- **Full enterprise-class security features for the remote teleworker**

Cisco Systems engaged Miercom to evaluate the Enterprise-class Teleworker (ECT) solution. ECT is a highly scalable Cisco IOS Software solution that securely integrates network and management infrastructures and applications all within a single device.

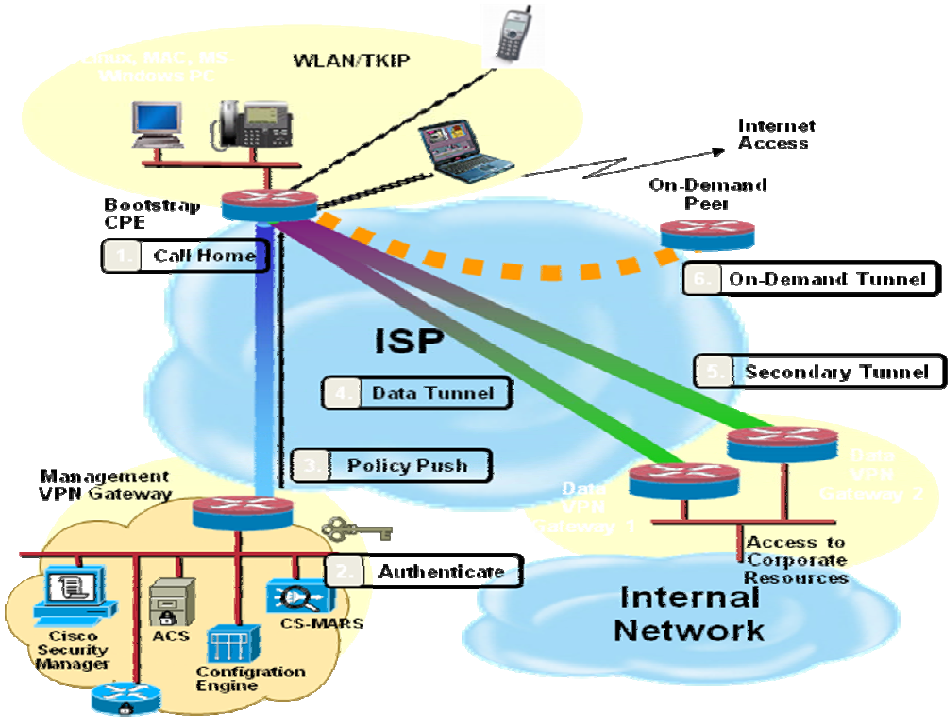
ECT allows customers to extend the full class of enterprise service to the remote office and teleworkers. The zero-touch deployment design lowers the barrier of resource requirements while enhancing the manageability and allows for increased productivity for IT staff.

Cisco's ECT provides an easy to manage, simple to deploy, secure solution for remote workers. The solution takes into account low overhead centralized management for large scale deployments and home user requirements of guest access and ease of use. Layered on top is security through every step of the process to ensure Enterprise networks are not compromised.



Cisco ECT provides secure Enterprise access for teleworkers with minimal setup and disruption of users home networks.

Test Set-up



Devices Under Test - Test Bed:
Testing was performed with a Cisco 871 wireless router running IOS software version 12.4(9)T3 on the remote side. This established a connection with a Cisco 3845 Integrated Services Router (ISR) with an AIM SSL/3 encryption card on the server side. Connections were made over the public Internet. Additional equipment on the server side of the network included: Cisco Security Manager server, Cisco Secure ACS server, Public Key Infrastructure (PKI) Certificate server, Configuration Engine server.

To enable testing, the end user router was created as a device within the Cisco Security Manager which included a respective ECT security policy as well.

For voice testing Cisco 7980 Series Video phones were used to place calls. The phones were register to a Cisco Call Manager v6.0 located on the server side of the network.

Additional details of the test environment required such as additional network components exact names and hardware versions, server version numbers, etc.

Configuration

Physical Configuration

The Cisco 871 router is a small Integrated Services Router (ISR) targeted for the small and home office environments. It is fixed configuration and features a 10/100 Mbps uplink with an integrated 4-port 10/100 Mbps managed switch. It can also be purchased with 802.11b/g support for wireless access.

Software Configuration

With the Cisco 871 there are several security features integrated as part of Cisco IOS including: Stateful Inspection Firewall, IPSec VPNs, SSL, Intrusion Prevention System, VLAN support and 802.1x authentication support. The 871 also supports Advanced QoS features.

Test Results

Testing started with an existing infrastructure and a factory sealed Cisco 871 wireless router. The unit was opened and connected to the network as an enterprise-class teleworker would. Once connected, a number of different services and functions were verified.

Zero Touch Deployment

Out of the box, the Cisco 871 router had a factory installed default configuration. With a single sheet of instructions, the router was quickly configured and connected to the enterprise network. The first step involved configuring the router to establish basic Internet connectivity using the Secure Device Management (SDM) wizard. SDM is a secure web-based wizard that walks the end user through a very straight forward set of instructions to setup

user credentials, indentify the type of broadband connection and set the basic security policies for the router. The Internet connection was established over an SSL link and demonstrated that security was applied throughout the entire process.

Once Internet connectivity was established, a second step involved securely triggering the remote provisioning process. Again using a secure web browser connection, a tunnel was established with the corporate VPN server and the final configuration, security settings and certificates were all downloaded. This was achieved using Cisco's Secure Device Provisioning (SDP) IOS feature, where a PKI certificate and the router bootstrap configuration were securely deployed.

Simple, secure management
For provisioning, administrators need only to create a profile for users in the Cisco Secure ACS database. The ACS tool automatically creates the required configuration file for when the user first connects the router to the network. Within the test database, a previous existing device was used as the template to quickly create a new user profile. Profiles can also be created from scratch.

When the users first connect to the VPN server, in addition to a having a valid PKI certificate, they must also have a valid ACS profile. Prior to the creation of the profile, the test unit could not log in, even with a valid PKI certificate. This combination of security validation ensures that both the router and the user are authorized to connect to the corporate network.

Remote Host Security
The Cisco 871 supports VLANs on the integrated switch. By default, devices connected to the switch are placed into a guest VLAN. When a PC was configured with 802.1x authentication and successfully verified, it was placed into the corporate VLAN and able to connect to the corporate network.

Using `PING` and `TRACEROUTE`, non 802.1x authenticated PCs were verified, and only had access to the Internet. Those PCs that successfully verified with 802.1x could connect to the corporate network for the appropriate data requests while Internet requests were served local via split-tunneling.

The splitting of guest or home traffic and corporate traffic was also extended to the WLAN. Computers configured with EAP-FAST were able to access corporate data via the corporate VLAN while all other PCs were placed on the guest LAN and routed to the local Internet. The guest WLAN can also be configured with WEP or WPA-PSK to enhance security for local machines.

All of the VLAN assignments were automatic and dynamic based on the credentials presented. During testing, PCs were moved between ports on the Cisco 871 and the VLAN settings adjusted accordingly without user or administrative intervention.

Figure 1: Cisco 870 series router

QoS for Voice and Video
A Cisco 7980 Video phone was connected to the Cisco 871 router and upon detection automatically assigned to a designated VLAN and registered with the corporate Call Manager. As part of the initial configuration, the bandwidth available via the ISP was entered. This was then used to automatically set QoS variables to ensure optimal voice and video quality. During testing, calls were placed to a second video phone with background traffic. There was no perceivable degradation of quality during the call.

Dynamic VPN Tunnels
A call was placed between a Cisco 871 and a Cisco 1811 representing a branch office using two Cisco 7980 video phones. Examination of the routing and IPSec tables within both routers showed that a tunnel was dynamically created between the two spoke sites, optimizing the RTP traffic flow.

Conclusion

Cisco's ECT provides an easy to manage, simple to deploy, secure solution for the remote worker. The solution takes into account low overhead centralized management for large scale deployments, and home user requirements of guest access and ease of use. Layered on top is security through every step of the process to ensure Enterprise networks are not compromised.

Miercom Performance Verified

Based on Miercom's examination and testing of the Cisco Enterprise-Class Teleworker solution and review of its configuration, deployment and operation as described herein, Miercom hereby issues the Performance Verified certification for the product in this report. Miercom certifies the following key observations made during this review:

- **Enterprise-class teleworker (ECT) solution enabled through Cisco Integrated Services Router platforms**
- **ECT enables voice, video and data solutions for enterprise teleworkers**
- **Zero-touch deployment improves manageability and service roll out**
- **Full enterprise-class security features for the remote teleworker**

Cisco Systems, Inc
170 West Tasman Drive
San Jose, CA 95134 USA
www.cisco.com

Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

About Miercom's Product Testing Services…

With hundreds of its product-comparison analyses published over the years in such leading network trade periodicals as *Business Communications Review* and *Network World*, Miercom's reputation as the leading, independent product test center is unquestioned. Founded in 1988, the company has pioneered the comparative assessment of networking hardware and software, having developed methodologies for testing products from SAN switches to VoIP gateways and IP PBX's. Miercom's private test services include competitive product analyses, as well as individual product evaluations. Products submitted for review are typically evaluated under the "Net**WORKS** As Advertised™" program, in which networking-related products must endure a comprehensive, independent assessment of the products' usability and performance. Products that meet the appropriate criteria and performance levels receive the "Net**WORKS** As Advertised™" award and Miercom Labs' testimonial endorsement.

379 Princeton-Hightstown Rd., East Windsor, NJ 08512
609-490-0200 • fax 609-490-0610 • www.miercom.com

Report 071015