Key findings and conclusions:

- New Cisco 1841 modular router can load an E1-rate (2 Mbps) WAN link with 3DES-encrypted, VPN traffic
- Delivers high WAN throughput while also running firewall, QoS, IPS and other services
- Modular design, supports an array of plug-ins, including WAN-interfaces and switch modules
- Various security options including Dynamic Multipoint VPN (DMVPN), Easy VPN server

Cisco Systems engaged Miercom to independently verify configuration, operational and performance aspects of its new, modular 1841 Integrated Services Router.

The Cisco 1841 represents a next-generation evolution of the Cisco 1721 router. The Cisco 1841 is designed to deliver multiple services – including stateful firewall, VPN tunneling and encryption, and intrusion prevention system (IPS) in a single compact chassis. Also, various optional modules can augment the system’s feature and service repertoire and/or performance. For example, while the 1841 comes with an on-board hardware crypto processor that provides VPN acceleration using an optional IOS security image, encryption performance can be further increased with an Advanced Integration Module (AIM), as was the case in this test bed.

The 1841 ran a late-beta version of IOS 12.3(11)T in the test bed. Miercom verified that, while running various additional services (see table on page 3), the 1841 could sustain a bi-directional, E1-capacity IP WAN link, with a 3DES-encrypted, mixed traffic load (see below). This router is designed to deliver security and data services concurrently at full T1/E1 rates.

**E1 load.** Measurements found the 1841 router could process sustained throughput of nearly 2 Mbps over an E1 IP-WAN link. All data was QoS-classified, 3DES-encrypted and secured through Cisco’s Dynamic Multipoint VPN (DMVPN). The red line shows the max theoretical link capacity.
Mixed concurrent services, traffic flows. The SUT (System Under Test) was the new Cisco 1841 Integrated Services Router. A key objective was to verify that, with various services running, the 1841 could still effectively sustain high throughput – filling an E1 (2-Mbps) IP-WAN link. In the test bed, the 1841 router was connected via a 10/100 Ethernet, IEEE 802.1p/q-based VLAN trunk to a switch, supporting two LAN subnets. The 1841 connected via an IPsec VPN tunnel over an IP-WAN link with the “main office.”

A mix of concurrent traffic streams was generated to exercise the services running on the 1841, including QoS classification. All traffic from the LAN headed out to the IP-WAN had to be classified and queued, based on DSCP (DiffServe Codepoint) values. Traffic arriving via the WAN E1 had to be appropriately VLAN tagged and routed.

Traffic flows were generated to provide QoS diversity, and to demonstrate the 1841’s ability to load the E1 link, while processing all WAN traffic through “Triple-DES” (3DES)-encrypted, DMVPN tunnels. Ixia IxChariot traffic-generating systems (v4.3) were used, establishing multi-protocol, bi-directional traffic flows on two different subnets.

On one subnet the IxChariot generated: 2 two-way G.729 VoIP RTP streams (24 kbps each), 1 DNS, 1 HTTPS, 1 POP3, 1 SMTP, and 1 FTP sessions. The other IxChariot generated: 3 two-way G.729 VoIP RTP streams, 1 FTP, 1 HTTPS and 3 HTTP sessions.

The 1841 router was also supporting two different VPN configurations: Dynamic Multipoint VPN, which enables multiple site-to-site VPN tunnels, and Cisco’s Easy VPN server, where remote users running Cisco VPN Client software set-up up dynamic, IPsec-encrypted tunnels. In the test bed a Cisco “MultiClient Unity Tool,” v4.0, running on a Red Hat Linux platform, simulated multiple VPN clients connecting to the 1841.
Modularity and Concurrency

Our test bed validated the 1841, a small-branch-office router, as a compact (1RU) system that can assume many jobs, including those of several otherwise separate security appliances.

As the above table shows, the native IOS of the 1841 offers users key integrated security capabilities. Among them:

- Stateful Firewall
- In-line Intrusion Prevention System (IPS)
- VPN tunneling and encryption
- QoS

The stateful firewall provides dynamic control over ports and protocols, carefully limiting access from the outside. Also, while not used in this test bed, NAT is a collateral capability, which effectively protects internal IP addresses.

The in-line IPS capability inspects inbound traffic, applying hundreds of known attack “signatures” to spot and suppress threats.

Our test bed highlighted the 1841’s VPN capabilities. We verified DMVPN operation. VPN tunnels were set-up and run over the E1 IP-WAN link. We also exercised Cisco’s Easy VPN server, which lets remote users running the Cisco VPN Client software set-up dynamic, auto-negotiated IPsec-based tunnels.

With all the security services running, and more – including QoS processing and SLA Monitoring-based network and link monitoring – the 1841 could still sustain bi-directional E1-capacity. The 1841 is a powerful branch router, capable of delivering multiple concurrent services along with high-volume, encrypted WAN throughput.
Miercom Verified Performance

Based on Miercom’s thorough workout of this system – and examination of its configuration, operation and features, as described herein – Miercom proudly attests to this system’s performance, in particular:

• The 1841’s ability to load an E1 link, 3DES-encrypting nearly 2 Mbps of WAN traffic via Advanced Integration Module (AIM)-based hardware encryption module.

• Concurrent provision of key high-level network services to a busy branch or small office, including stateful firewall, and in-line IPS, while under heavy traffic load. Service Level Agreement monitoring was also verified.

• Support for varied VPN topologies and requirements. We verified the 1841’s support of Dynamic Multipoint VPN, as well as Cisco’s Easy VPN server, where remote clients running Cisco’s VPN software establish dynamic, auto-negotiated VPN tunnels.

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 “NetWORKS 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 “NetWORKS As Advertised™” award and Miercom Labs’ testimonial endorsement.