Miercom

Lab Testing Summary Report

April 2009

Report 090904

Product Category:

Aggregation Services Router Architecture & Performance

Vendor Tested:

CISCO

Products Tested:

Cisco ASR 1002, 1004 and 1006 Series Routers

Key findings and conclusions:

- **ASR1000-ESP20 module provides 20 Gbps of routing real world HTTP traffic, with firewall enabled**
- **Multi-gigabit performance of Network Based Application Recognition with Flexible Packet Matching for Deep Packet Inspection and filtering**
- **ASR 1004/1006 provides up to 6 Gbps encrypted throughput with tunnel-less GETVPN technology**
- **Exceptional WCCPv2 redirection performance, WAAS software improves data optimization by 30%**

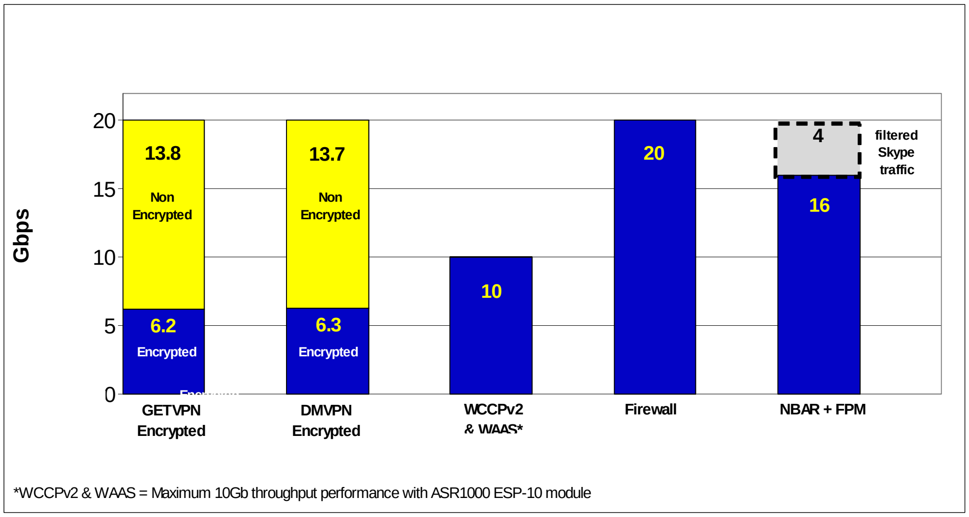
Cisco ASR 1002, 1004, and 1006 Aggregation Services Routers were reviewed for advanced features, scalability, and throughput performance. We tested Cisco IOS Group Encrypted Transport VPN (GETVPN), Dynamic Multipoint Virtual Private Network (DMVPN/Qos), Flexible Packet Matching (FPM), Network Based Application Recognition (NBAR) and Wide Area Application Services (WAAS) based WAN head-end optimization features.

This is the second part of in-depth testing of the Cisco ASR 1000 family of Aggregation Service Routers. All of the tested features were enabled on ESP modules. The 20-Gbps ASR Series Embedded Service Processor (ASR1000-ESP20) module is used on ASR 1004/1006 chassis. ESP20 provides 20 Gbps bandwidth and supports hardware assisted policing and an encryption capability of 8 Gbps. For use on the ASR 1002 the ASR1000-ESP5 allows 5 Gbps bandwidth and encryption capability rated at 1.8 Gbps. ASR1000-ESP10 module has 10 Gbps bandwidth with encryption capability of 4 Gbps. This module works with any of the ASR 1002/1004/1006 chassis.

During the first phase of testing in May 2008, shown in Figure 1, the focus was on base line performance, *(continued on page 3)*

Figure 1 ASR 1000 series - Performance Throughput

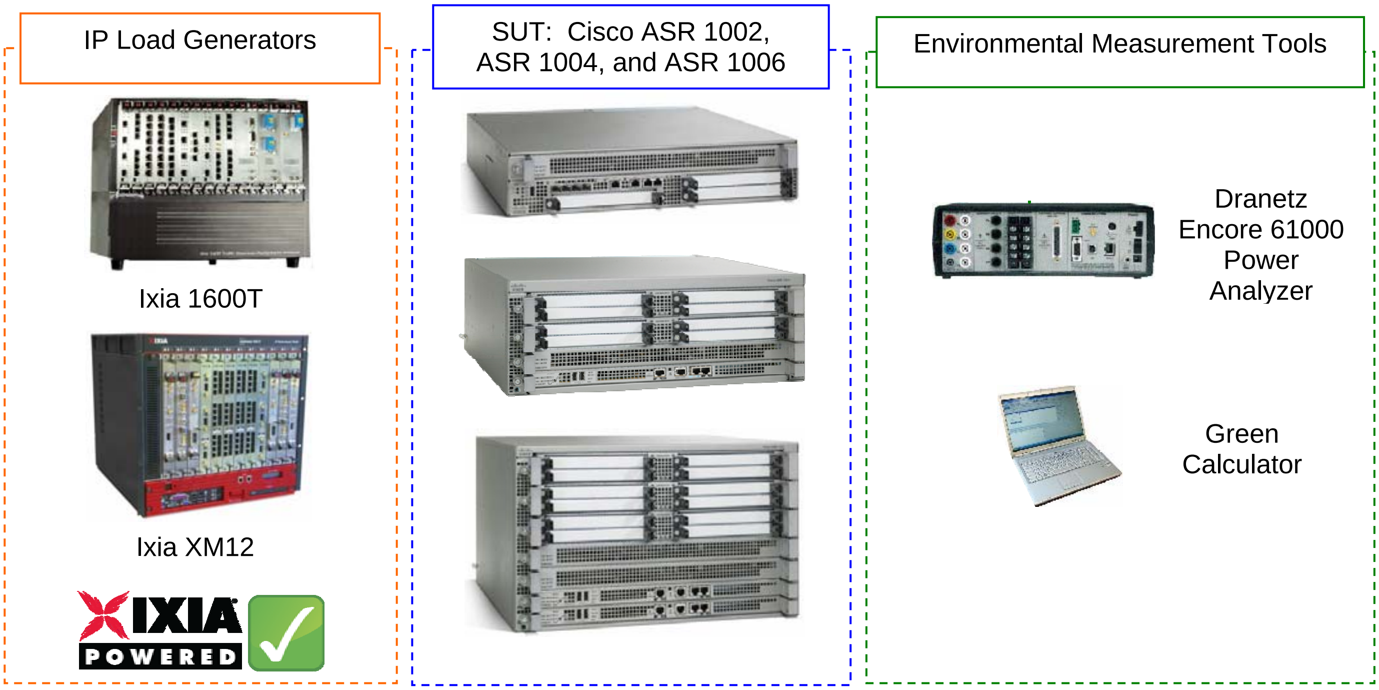
Throughput performance with encrypted traffic, application acceleration, firewall, and deep packet filtering features enabled



*WCCPv2 & WAAS = Maximum 10Gb throughput performance with ASR1000 ESP-10 module

Cisco ASR 1006 with ASR1000-ESP20 module achieved over 6 Gbps encrypted traffic and 20 Gbps was observed with firewall enabled. 4 Gbps Skype traffic was filtered out of a 20 Gbps stream, with no packet loss of desired traffic. 10 Gbps was achieved with ASR 1000 ESP10 for application acceleration.

Test Bed Diagram



How We Did It

Cisco ASR 1000 series of Aggregation Services Router was evaluated for its performance by looking at the architectural design and the different services and features offered by the router solution. Services and features observed were Secure VPN without the need of tunneling, Dynamic Multifunction VPN, scalability and performance of the midrange crypto head-end with WCCPv2 and WAAS, integrated thread control and the WAN optimization platform.

Lab testing of each architectural performance feature was conducted under maximum load. The ASR 1002 was configured with the following components: ASR1002-SIP10, ASR1000-ESP10 module, ASR1002-RP1 module, two SPA-1X10GE-L-V2 modules, SPA-2X1GE-V2 module and dual PSUs. The ASR 1004 was configured with two ASR1000-SIP10 modules, ASR1000-ESP20 module, ASR1000-RP1/RP2 module, three SPA-1X10GE-L-V2 modules, SPA-10X1GE-V2 module, and dual PSUs.

Configuration for the ASR 1006 included two ASR1000-SIP10, ASR1000-ESP20 module, two ASR1000-RP1/RP2 modules, three SPA-1X10GE-L-V2 modules, two SPA-10X1GE-V2 modules, SPA-4XOC3-POS module, SPA-2XCT3/DS0 module, and dual PSU. When the SUT was configured with ASR1000-RP2, we tested GETVPN to verify higher tunnel per-second rate. For GETVPN and DMVPN IOS release 2.3.0 was used. For IOS firewall, FPM, NBAR, and WCCP2 technologies, IOS XE release 2.2.2 was used.

Ixia XM12, Ixia 1600T, and Ixia 400T traffic generators from Ixia (www.ixiacom.com) were employed to obtain a range of throughput traffic, vary the traffic load, and utilize varying processor rates. Real-world traffic was generated by Ixia's test platform and test applications such as IxNetwork, IxLoad, and IxAutomate for Layer 2-3 routing and switching traffic.

Ixia is an industry leader in energy efficiency testing of networking equipment. Ixia's unique approach utilizes coordination of energy measurements with network traffic load – allowing energy consumption to be graphed against network traffic volume. Real-world traffic is generated by Ixia's test platform and test applications, principally IxNetwork for Layer 2-3 routing and switching traffic and IxLoad for Layer 4-7 application traffic.

(continued from page 1) with features enabled such as ACL + uRPF, Crypto, and firewalls. See Figure 1 fo a summary of all testing performed. A Cisco ASR 1006 router with ASR1000-ESP10 module was used. Details of part one testing (Report 080509) is available at http://www.miercom.com/cisco.

The Cisco ASR 1000 series routers are also the recipients of Miercom Certified Green Award. Green certification was awarded for their energy-saving attributes which were evaluated in December 2008 by Miercom in accordance with the Certified Green Testing Methodology.

Tunnel-less Secure VPN

Today's network environment needs to support all forms of media including data, voice and video, for business communications. Voice and video applications are accelerating the need for instantaneous, branch-to-branch communications. In most cases, this can create increased risk in network security. To address these new challenges, an organization needs an intelligent network that securely integrates applications in a way that is easy to manage. The Cisco ASR 1000 series routers continues to provide Group Encrypted Transport VPN (GETVPN), which offers optimum bandwidth efficiency while securing communications by managing an encrypted VPN that does not require tunnels.

For this test, two Cisco ASR 1006 routers, each with the ASR1000-ESP-20 module, were utilized as the connection between two Group Members (GM). After applying IMIX traffic (58% at 64bytes, 34% at 570bytes, and 8% at 1400bytes), crypto throughput was 2.7 Gbps unidirectionally. Bidirectional equals a frame transfer rate of 5.5 Gbps total crypto throughput at the Group Members, without any packet loss.

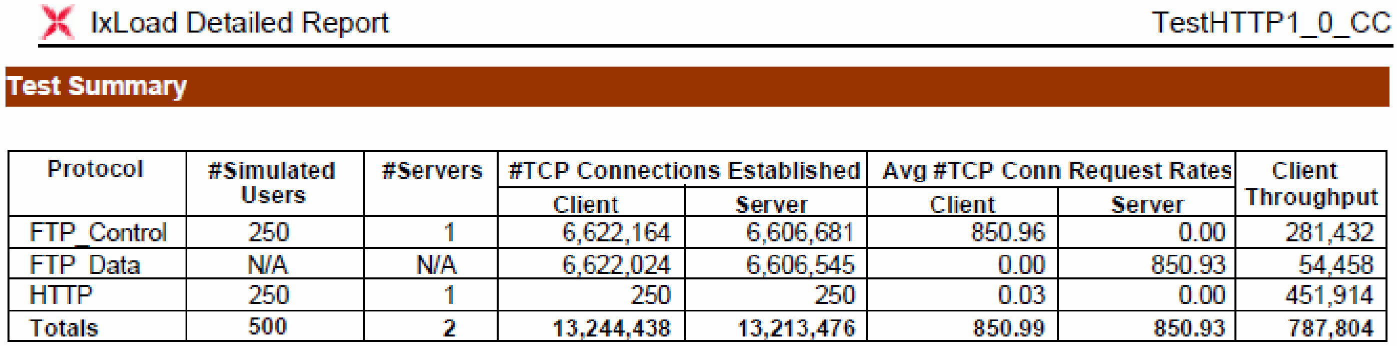
Dynamic Multipoint VPN

The Dynamic Multipoint Virtual Private Network (DMVPN) is an enhancement of the VPN configuration process of Cisco IOS-based routers. DMVPN prevents the need for pre-configured/static IPsec peers in crypto-map configurations. An IPsec tunnel between two Cisco ASR 1000 series routers may be created on an as needed basis. Tunnels may be created between a spoke router and a hub router (VPN head-end), or between spokes. This alleviates the need for the hub to route data between the spoke networks, a commonly found meshed frame relay topology.

In order to test Dynamic Multipoint VPN one Cisco ASR 1006 with head-end function enabled and four physical spokes, each simulating 250 virtual spokes or branch offices with both unicast and muilticast traffic were utilized in the test bed. The multiple virtual branches were simulated using Cisco C7200 and ASR 1000 series routers. Tunnels were established between the hub and the spoke routers. During this test, both Ixia IxNetwork and IxExplorer provided unicast and multicast traffic at IMIX rates. When IMIX rate traffic was started on the ASR 1006 with an ASR1000-ESP-20 module, 5.2 Gbps before encryption and 6.3 Gbps post encryption of traffic was observed.

Some benefits of Dynamic Multipoint VPN include Hub Router Configuration Reduction, whereby a configuration on the hub router defines the crypto map characteristics, the crypto access list, and the Generic Routing Encapsulation (GRE) tunnel interface. This feature allows users to configure a single mGRE tunnel interface, a single IPsec profile, without crypto access lists on the hub router to handle all spoke routers.

Figure 2 Application Acceleration



IxLoad Detailed Report TestHTTP1_0_CC

Test Summary

Protocol	#Simulated Users	#Servers	#TCP Connections Established		Avg #TCP Conn Request Rates		Client Throughput
			Client	Server	Client	Server	
FTP_Control	250	1	6,622,164	6,606,681	850.96	0.00	281,432
FTP_Data	N/A	N/A	6,622,024	6,606,545	0.00	850.93	54,458
HTTP	250	1	250	250	0.03	0.00	451,914
Totals	500	2	13,244,438	13,213,476	850.99	850.93	787,804

Details of an IxLoad report for 250 FTP and 250 HTTP clients using WCCPv2 with full optimization enabled. Each FTP and HTTP client requested 64KB and 4KB objects respectively. More than thirteen million TPC connections were established between servers and clients.

Another benefit is Automatic IPsec Encryption Initiation, where the GRE has the peer source and destination address configured or resolved with NHRP. This feature allows IPsec to be immediately triggered for the point-to-point GRE tunneling, or when the GRE peer address is resolved via NHRP for the multipoint GRE tunnel. An additional benefit is the dynamic creation for spoke-to-spoke tunnels. When a spoke router transmits a packet to another spoke router, it can utilize NHRP to determine the required destination address of the target spoke router.

Scalable Data Optimization

Web Cache Communication Protocol Version 2 (WCCPv2) gives the ASR 1000 series the ability to intercept and redirect network traffic to a nearby network device running Cisco WAAS software, for purposes of application acceleration and WAN optimization. By using WCCPv2 with WAAS and the Cisco Wide Area Application Engine (WAE) hardware platform, IT organizations can optimize network flows, file access, applications and other content. The Cisco WAAS egress methods streamlines and simplifies WCCPv2 deployments. Cisco WAEs can reside on the same subnet as users or servers and in the same address space.

Scalability and performance testing of the Cisco ASR 1000 with WCCPv2 and WAAS enabled, was conducted using one Cisco ASR 1006 router with WAN head-end enabled. Additionally, three Cisco C7200s and one Cisco ASR 1004 router were used to simulate four spokes. Each spoke simulated a branch office. Multiple WAEs were required in order to measure the collecting WCCPv2 intercepted bandwidth from the Cisco ASR 1006 router. Both L2/L2 and GRE/GRE methods were observed when testing WCCPv2 throughput on the DUT. Refer to Figure 2.

	Baseline		WCCPv2 L2/L2		WCCPv2 GRE /GRE redirect	
Packet size	NDR Mpps	QFP NDR Mpps	NDR Mpps	QFP NDR Mpps	NDR Mpps	QFP NDR Mpps
64B	~ 10Gb	14.88	9408	14	7542	7.6
128B	~ 10Gb	8.3	9827	8.6	8361	8
256B	~ 10Gb	4.5	9715	5.6	9181	5.3
IMIX	~ 10Gb	3.3	9873	4.3	9349	4.7
512B	~ 10Gb	2.2	9863	2.9	9527	2.8
1500B	~ 10Gb	0.8	9849	0.9	9769	1.7

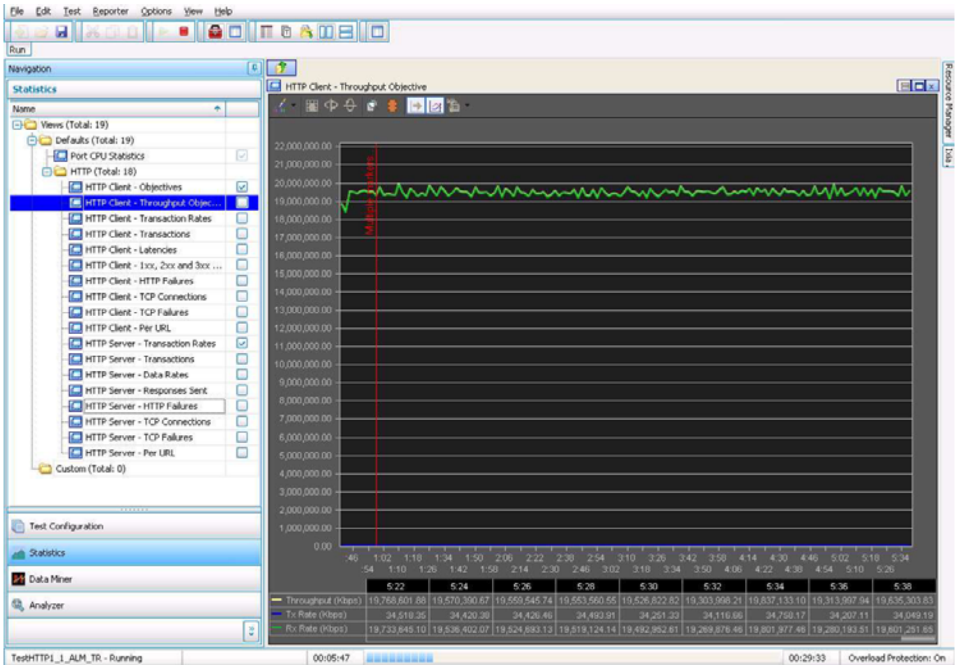
The total Non Drop Rate (NDR) throughput with WCCPv2 performance enabled for both L2/L2 and GRE/GRE methods, were better in comparison to baseline performance.

Integrated Threat Control

For this test, a Cisco ASR 1006 router with four 10 Gbps SPA modules was used as the Internet Gateway Router and Integrated Threat Control with IOS Zone Policy Firewall was configured. IxLoad was used to simulate the HTTP traffic of four servers and four clients, each with line rate of 10 Gbps. A max of 1,048,582 current sessions, as

Figure 3 Firewall Enabled

The IxLoad Firewall diagram shows the total throughput once the Integrated Threat Control with IOS Zone Policy firewall was enabled. It reached 20 Gbps, once Layer 3 overhead was added to total throughput on the Cisco ASR 1006 router. Zero packet loss was observed.



	5:22	5:24	5:26	5:28	5:30	5:32	5:34	5:36	5:38
Throughput (Kbps)	19,768,601.88	19,570,390.67	19,559,545.74	19,553,560.55	19,526,822.82	19,303,998.21	19,837,133.10	19,313,997.94	19,635,303.83
Tx Rate (Kbps)	34,518.35	34,420.38	34,426.46	34,493.91	34,251.33	34,116.66	34,758.17	34,207.11	34,049.19
Rx Rate (Kbps)	19,733,645.10	19,536,402.07	19,524,693.13	19,519,124.14	19,492,952.61	19,269,876.46	19,801,977.46	19,280,193.51	19,601,251.65

well as a max of 270,000 sessions per second were observed, with a total firewall throughput with TCP/UDP inspection of 20 Gbps, once Layer 3 overhead was taken into account. Refer to Figure 3 for firewall enablement.

Deep Packet Inspection

Network Based Application Recognition (NBAR) is a mechanism used by the Cisco ASR 1000 series to recognize a dataflow by the first packet sent. NBAR does a deep packet inspection on the first packet, to determine which traffic category the flow belongs to. QuantumFlow Network Processor is used to handle this flow appropriately. The ability of NBAR to recognize dataflow by a packet is useful in dealing with malicious software that uses known ports to fake "priority traffic", as well as non-standard applications using dynamic ports. On the ASR 1000 series routers, NBAR is mainly used for Quality of Service and security purposes.

Cisco ASR 1000 series with NBAR enabled gives network administrators the ability to see the variety of protocols and the amount of traffic for each protocol. This can then be used to provide different levels of service for network traffic.

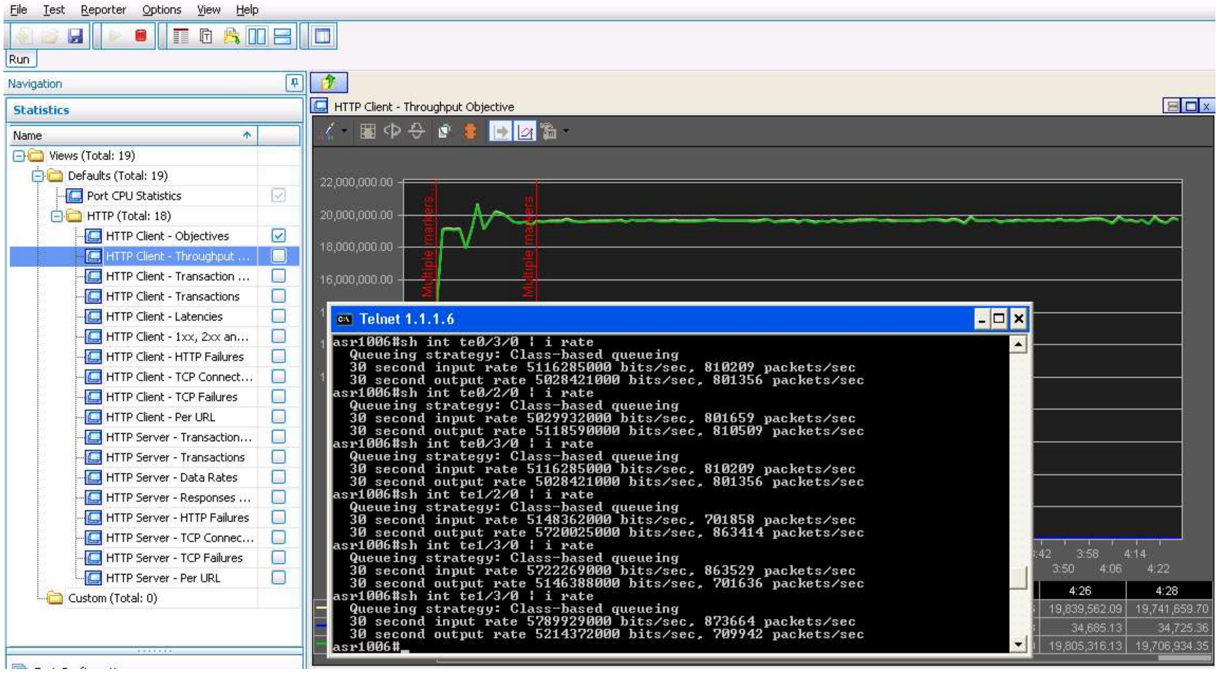
During this test, the Cisco ASR 1006 was used at the Internet Edge. NBAR was configured with QoS policies. We focused on verification of HTTP traffic with the native QFP acceleration and documented the classification results with 64KB HTTP object size. IOS FPM (Flexible Packet Matching) testing was used as a filter to block most of the worm attacks, once the attack vector had been identified. For this test, the router was configured to block any TCP based Skype connection attempts. Once the Cisco ASR 1006 router started matching the pattern for Skype type traffic, all packets related to Skype traffic were dropped as previously configured on the NBAR. See Figure 4. The Cisco ASR 1006 router was able to sustain, filter and drop worm-attacks on the 20 Gbps line rate traffic at 128-Byte packets even with deep inspection enabled.

The Cisco ASR1000-ESP20 module enhances the performance and functionality of the ASR 1000 series routers. With this enhanced functionality, the ASR1000-ESP20 module provides multi-gigabit performance on NBAR an FPM combined, as well as encrypted tunnel-less VPN connectivity.

Bottom Line

ASR 1000 series routers, while using the appropriate ESP module, has many advanced features. During the performance and throughput tests with and without encryption, multi-gigabit rates were achieved, allowing WAN optimization, while using VPN.

Figure 4 Deep Packet Inspection - ASR 1006



```
asr1006#sh int te0/3/0 | i rate
  Queueing strategy: Class-based queueing
  30 second input rate 5116285000 bits/sec, 810209 packets/sec
  30 second output rate 5028421000 bits/sec, 801356 packets/sec
asr1006#sh int te0/2/0 | i rate
  Queueing strategy: Class-based queueing
  30 second input rate 5029932000 bits/sec, 801659 packets/sec
  30 second output rate 5118590000 bits/sec, 810509 packets/sec
asr1006#sh int te0/3/0 | i rate
  Queueing strategy: Class-based queueing
  30 second input rate 5116285000 bits/sec, 810209 packets/sec
  30 second output rate 5028421000 bits/sec, 801356 packets/sec
asr1006#sh int te1/2/0 | i rate
  Queueing strategy: Class-based queueing
  30 second input rate 5148362000 bits/sec, 701858 packets/sec
  30 second output rate 5720025000 bits/sec, 863414 packets/sec
asr1006#sh int te1/3/0 | i rate
  Queueing strategy: Class-based queueing
  30 second input rate 5722269000 bits/sec, 863529 packets/sec
  30 second output rate 5146388000 bits/sec, 701636 packets/sec
asr1006#sh int te1/3/0 | i rate
  Queueing strategy: Class-based queueing
  30 second input rate 5789929000 bits/sec, 873664 packets/sec
  30 second output rate 5214372000 bits/sec, 709942 packets/sec
asr1006#
```

Using IxLoad, Cisco ASR 1006 shows 20 Gbps throughput after Skype traffic packets were blocked, utilizing NBAR. There were no QFP Global drops detected during testing of the ASR 1006.

Miercom Performance Verified

Based on Miercom's review of the Aggregation Services Routers, the Cisco ASR 1000 series routers are awarded Performance Verified in the 2009 Miercom Router Industry Assessment.

Miercom Performance verified is awarded to Cisco for:

- **Improved data optimization with WAAS software**
- **6 Gbps encrypted throughput with GETVPN**
- **Provides 20 Gbps of routing HTTP traffic with firewall enabled**

**Cisco ASR1002,
ASR1004, and ASR 1006**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134
www.cisco.com
1-800-553-6387

About Miercom's Product Testing Services

Hundreds of product-comparison analyses have been published over the years in such leading network trade periodicals as Network World, Business Communications Review - NoJitter, Communications News, xchange, Internet Telephony and other leading publications. Miercom's reputation as the leading, independent product test center is unquestioned.

Miercom's private test services include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable, Certified Reliable, Certified Secure and Certified Green. Products may also be evaluated under the NetWORKS As Advertised program, the industry's most thorough and trusted assessment for product usability and performance.

Before printing, please consider electronic distribution

Product names or services mentioned in this report are registered trademarks of their respective owners. Miercom (Mier Communications, Inc.) makes every effort to ensure that information contained within our reports is accurate and complete, but is not liable for any errors, inaccuracies or missions. Miercom is not liable for damages arising out of or related to the information contained within this report.