Im Test – Cisco Catalyst 6500

Von Bernd Klusmann

Bild: EANTC

Das herstellerunabhängige Berliner Testlabor EANTC ermittelte die Leistung, Funktionalität und Brauchbarkeit der neuen Content-Switching- und Firewall-Module für den Cisco Catalyst 6500. Die Tests wurden mit Ixia's Ixload-Applikation durchgeführt. Ixia beauftragte EANTC mit der Evaluierung.

Cisco Systems trug nicht zur Finanzierung der Messungen bei, sondern stellte lediglich das zu testende System inklusive Konfigurations-Support zur Verfügung. Der Catalyst war ausgestattet mit einer Supervisory Engine 720 sowie mit 48-Port-Ethernet- (10/100/1.000), Content-Switching- und Firewall-Module. Bei Ixload handelt es sich um eine Applikation, die realitätsnah Hochleistungs-Web-Traffic generiert und analysiert. Damit ist es möglich, realistische Verkehrsszenarien auf TCP- und Application-Layern zu simulieren.

Test-Methodik und Konfiguration

EANTC verwendete die Performance-Testpläne des IETF: Benchmarking Terminology for Firewall Performance (RFC 2647) sowie Benchmarking Methodology for Firewall Performance (RFC 3511). Diese wurden wenn nötig angepasst, um die Tests auf der Anwendungsschicht zu spezifizieren. Die emulierten Server und Clients wurden mit 46 Gigabit-Ethernet-Ports an den Catalyst 6509 angeschlossen. Um DDoS-Angriffe einzuspeisen, kam ein Fast-Ethernet-Port zum Einsatz.

Bernd Klusmann ist Projektmanager beim EANTC. Er leitet Tests bei Unternehmenskunden und Serviceprovidern.

EANTC führte sechs Tests mit jeweils zwei unterschiedlichen Konfigurationen des Catalyst durch. Die erste Konfiguration stellte ein reguläres Firewall-Szenario für große Unternehmen dar, wobei nur das Firewall-Service-Modul (FWSM) zum Einsatz kam. Für das zweite Szenario, eine typische Rechenzentrumskonfiguration, wurde das Content-Switch-Modul (CSM) in den Datenweg zwischen Clients und Server eingesetzt. Das CSM schaltete Anschlüsse zu den unterschiedlichen Serverfarmen, basierend auf unterschiedlichen Protokollinformationen der Schicht 4 bis 7 wie URL-Inhalt oder TCP-Ports.

Geschwindigkeit und Anzahl von HTTP-Verbindungen

Im ersten Test (HTTP Session Capacity Performance) verifizierten die Experten die maximale Anzahl von gleichzeitigen Webanfragen (HTTP-Verbindungen). Dafür kamen bis zu 90.000 simulierte Nutzer und 23 simulierte Webserver zum Einsatz.

Ergebnis: Die Tester erzielten maximal 999,900 simultane HTTP-Verbindungen in beiden Szenarien, der Firewall- und der CSM-Konfiguration.

Die Analyse der HTTP Session Rate Performance zeigte, wie schnell die getestete Catalyst 6500 Konfiguration neue HTTP-Sitzungen fehlerfrei verarbeitet. Dafür erzeugte Ixload HTTP-Requests für 23 Server-IP-Adressen, 1.000, 10.000 und 50.000 Client-IPs mit 10.000, 50.000 und 90.000 Anwender.

Ergebnis: Ohne das Content-Switch-Modul konnte ein Spitzendurchsatz von 88.753 Sitzungen pro Sekunde erreicht werden. Mit dem CSM lag das beste Resultat bei 74.637 Sitzungen pro Sekunde.

Schutz vor DDoS Angriffen

In einer weiteren Phase wurde die Leistung des Systems gemessen, während es gleichzeitig aktiv DDoS-Attacken (Distributed Denial of Service) verhindert. EANTC wertete aus, in wie weit die Gesamtleistung beim Erreichen der Höchstzahl gleichzeitiger HTTP-Sessions beeinflusst wird. Dabei wurde die dafür benötigte Zeit ohne Angriff, sowie mit einem Angriff verglichen. Die Testparameter sind: 50.000 Client- und 23 Server-IPs sowie 50.000 Nutzer.

Ergebnis: Die DDoS-Angriffe zeigten keinerlei Auswirkungen auf die Leistung des Catalyst 6509. Während der Tests zeigte der Catalyst keinen signifikanten Anstieg der CPU- oder Speicherbelastung.

FTP-Durchsatz

Eine Analyse des maximalen FTP-Durchsatzes überprüfte die höchstmögliche Anzahl gleichzeitig aktiver FTP-Verbindun-

gen, die das getestete System beibehalten kann. Ixload simulierte dafür 23 Client- und 23 Server-Ports, 46.000 Client-IP-Adressen und 460.000 Nutzer.

Ergebnis: Tests mit beiden Konfigurationen erreichten das durch das Messgerät bedingte Maximum von 460.000 gleichzeitigen FTP-Sessions. Laut Cisco Systems sollen beide Switch-Konfigurationen jeweils eine Million gleichzeitiger Verbindungen bewältigen. Um den Catalyst an dieses Limit heranzuführen, hätte EANTC die Testhardware um den Faktor zwei erweitern müssen, da zur Zeit jeder Ixia-Port nur eine maximale Performance von 20.000 zeitgleichen FTP-Verbindungen aufweist.

Firewall-Regeln und Lastverteilung

In einem weiteren Test wurde die erreichbare Bandbreite des Firewall-Service-Moduls bei einer steigenden Anzahl von aktiven Firewallregeln (ACL, Access-List-Einträge) gemessen. Dabei belief sich die Zahl dieser Regeln auf 0, 10.000, 30.000 und 60.000. Zum Einsatz kamen 10.000 Client-IP-Adressen und ebenso viele Anwender sowie 23 Server-IPs.

Ergebnis: Das Catalyst-Firewall-Modul war in der Lage, bis zu 60.000 Firewall-Regeln ohne jeglichen Leistungseinbruch zu verarbeiten. Verglichen mit den Leistungsangaben, die ohne Firewall-Nutzung erzielt wurden, zeigen die Resultate mit den verschiedenen Regel-Sätzen keine bedeutende Abweichung.

Zuletzt analysierte EANTC die Leistung des Catalyst 6500 bei der Lastverteilung von HTTP-Verbindungen auf verschiedene Serverfarmen, basierend auf unterschiedlichen URL-Typen. Dafür setzten die Tester drei verschiedene URL-Typen ein (*.wav, *.jpg und *.htm), jeweils mit einer Länge von 128 Byte. Mit dem Ixia-Lastgenerator wurden HTTP-Verbindungen für 1.000, 10.000 und 50.000 Client- sowie 23 Server-IPs aufgebaut und 10.000, 50.000 sowie 90.000 Nutzer simuliert. Die Experten des EANTC-Testlabors konfigurierten drei Server-Gruppen, wobei jede Gruppe nur einen URL-Typ bediente. Der Testverkehr bestand aus einer ausgewogenen Mischung der drei Gruppen.

Ergebnis: Wie erwartet, verringert sich die Gesamtleistung für den HTTP-Verbindungsaufbau um 40 Prozent, wenn der Cisco Catalyst 6500 den Verkehr auf Layer 7 analysiert und diesen mit bestimmten Filterrichtlinien für weitere Versandentscheidungen vergleicht.

Ergebnis-Übersicht

Nr.	Test-Bereich	Ergebnis
1	HTTP Session Capacity Performance	✔
2	HTTP Session Rate Performance	✔
3	DDoS Prevention Performance	✔
4	FTP Concurrent Session Capacity	✔
5	Rule Set Based Performance	✔
6	HTTP Load Balancing Based on URL	✔

Fazit

Mit den neuen Content-Switch- (CSM) und Firewall-Service-Modulen (FWSM) hat Cisco leistungsfähige Komponenten für mittlere bis große Unternehmen und Serviceprovider ins Programm aufgenommen. Die Tests des EANTC zeigten, dass ihre Leistung und Skalierbarkeit auch für recht große Webserverfarmen beziehungsweise umfangreiche Firewall-Konfigurationen mehr als ausreicht. Das System war auch durch aggressive Angriffe gegen die Sicherheitsfunktionen nicht zu beeindrucken. Lediglich bei der Lastverteilung in Webserverfarmen erreichten wir die Leistungsgrenze. Besonders interessant ist die Integration in die weit verbreitete Catalyst-6500-Plattform, die eine flexible Konfiguration der Schnittstellen und weiteren Funktionen ermöglicht. *(CK)*