PERFORMANCE
TESTING
RESULTS

Trend Micro Web and Email Security Solutions on Crossbeam X80 Platform

Opus One
April 2008

Opus One conducted performance tests on two Trend Micro products—InterScan™ Messaging Security Suite and InterScan™ Web Security Suite—running on Crossbeam® X-Series platform. The goal of these tests was to determine the performance for the combined Trend Micro and Crossbeam solutions.

Testing of InterScan Web Security Suite on a fully populated Crossbeam X80 platform with 10 Application Processing Modules (APMs) returned performance of over 2.4 Gbps scanning HTTP traffic for viruses and spyware. This high level of performance demonstrates that the combination of Trend Micro InterScan Web Security Suite and Crossbeam Systems X80 platform is capable of ensuring web security for data centers, carriers, and the world's largest enterprises.

Testing of InterScan Messaging Security Suite on a fully populated Crossbeam X80 platform was capable of scanning 600 messages per second for viruses and spam, and 750 messages per second for viruses alone. With Trend Micro Email Reputation deflecting 76% of spam, the Crossbeam X80 could handle a load of up to 1645 messages per second, or an astonishingly high 140 million messages in a 24 hour period.

Overview

Crossbeam Systems builds network security platforms. The largest is the X80 platform, a 14-slot chassis running Crossbeam's own network operating system with high availability, load balancing, dynamic routing, and package management built into the platform. The X80 chassis can support up to 10 application processing modules (APM), each of which can be dedicated to a particular security application or grouped together to run one application.

InterScan Web Security Suite from Trend Micro is a software-based web security product for malware blocking, content filtering, and URL filtering. Trend Micro's InterScan Messaging Security Suite is an email security gateway solution with anti-spam, anti-virus, and other policy-based security features.

Crossbeam Systems, in conjunction with their partner Trend Micro, offers a chassis-based solution for Internet security which integrates the InterScan Messaging and/or InterScan Web security applications with X-Series XOS™ software, load balancing, and application management tools.

We tested the Crossbeam/Trend Micro solution using test equipment from Spirent. Although the test equipment was provided by Crossbeam, Opus One was responsible for all configuration and all test plans, as well as performing the tests and recording results. Crossbeam and Trend Micro staff were available during the test process and were responsible for installation of all Crossbeam and Trend Micro hardware and software. Opus One configured the InterScan Messaging Security Suite software and validated the configuration of the InterScan Web Security Suite software.

How We Tested InterScan Web Security Suite

The goal of web security performance testing was to determine the maximum performance possible in a typical enterprise or service provider deployment. InterScan Web Security Suite (IWSS) is capable of multiple security functions. For this test, we focused on the anti-virus and anti-spyware functions.

To measure performance, we loaded 10 different web objects (ranging in size from 1 KB to 1.5 MB) into the Spirent test equipment, including HTML (with embedded Javascript), GIF and JPEG images, PDF files, ZIP archives, and Windows executable files. No viruses or spyware were in the objects. The test equipment was configured to deliver this actual content from web servers to web clients in a mix of sizes and object types that approximates the Internet HTTP traffic of a typical enterprise.

InterScan Web Security Suite was loaded onto the Crossbeam X80 APMs and was configured by Trend Micro in a typical high performance configuration as a web proxy. An external log server was installed, and logs from the application were sent over the network to the log server. By default, InterScan Web Security Suite will scan objects smaller than 512 KB "in-line," and return an interstitial page to web clients for objects between 512 KB and 2 MB. This limit was raised so that no interstitial pages would be delivered to clients.

Four web client simulators, each using a single 1 GigE interface, were aggregated into a 10 GigE interface connected to the Crossbeam X80 chassis using a dedicated switch. Four similarly connected Spirent web server simulators were aggregated into a different 10 GigE interface using a second switch. The Spirent test equipment was configured to offer a load of up to 10,000 URLs/second, or approximately 4 Gbps, completely saturating the 4 Gbps network fabric in one direction.

To determine performance numbers, we ran a six minute test of web clients connecting through the IWSS proxy to web servers. Within the test, a constant three minute period was selected, and the actual throughput of the web clients was measured. Each test was repeated three times, and the average of the three results was reported. Rather than trying to convert measured bandwidth to some arbitrary number of users, the bandwidth numbers are presented here.

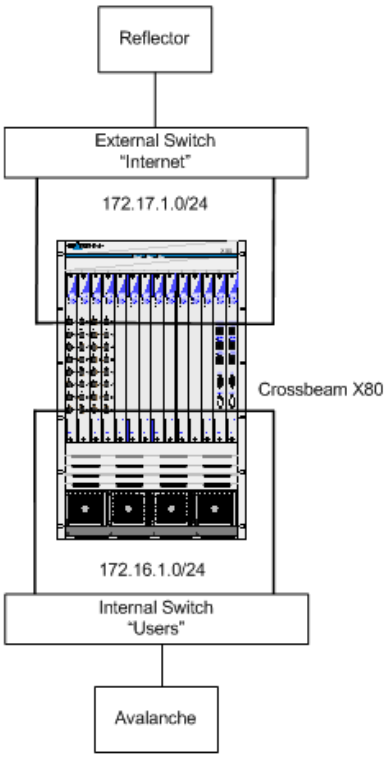

Figure 1: Test Bed

We did not test InterScan Web Security Suite URL filtering. URL filtering in most web security applications is an "in–the-cloud" function, where the web security application performs a real-time lookup against a reputation service. Because the most significant performance limit with reputation services is the speed of the reputation service and the Internet connection latency and speed, along with the response time of the reputation service, we did not feel that it would be possible to provide a meaningful or repeatable benchmark of this feature.

Results of Testing IWSS

Our testing of InterScan Web Security Suite showed that it was capable of processing loads from 346 Mbps with a single APM up to 2,419 Mbps with ten APMs. A chassis configured with "N+1" redundancy would be able to process peak loads of approximately 2,312 Mbps.

The performance numbers presented here should be considered as absolute maximum for peak levels of usage, and not as typical load limits. For example, with ten APMs and processing 2.4 Gbps of traffic, InterScan Web Security Suite introduced average latency of 168 milliseconds/URL, which we believe is near the outside limit of what would be acceptable to web users. A conservative sizing of the Trend Micro web Security/X80 combination would call for continuous load levels of between 50% and 75% of the limits presented in this test.

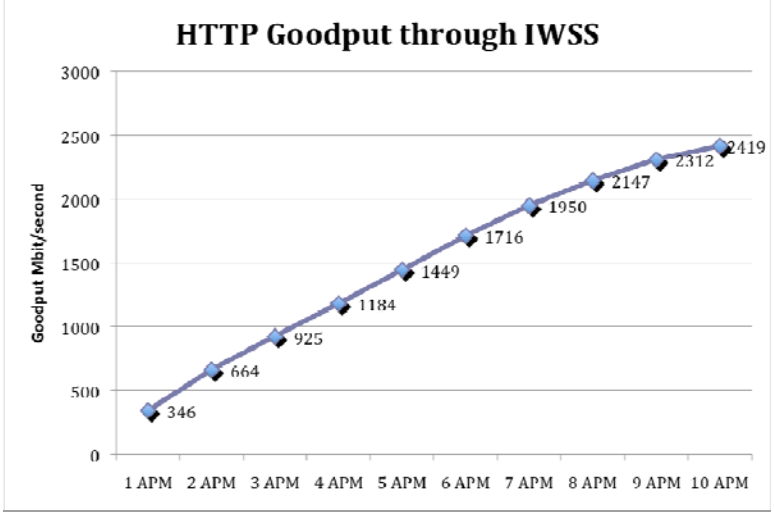

Figure 2: HTTP Goodput through IWSS

How We Tested InterScan Messaging Security Suite

The goal of the InterScan Messaging Security Suite (IMSS) test was to measure the steady-state capability of the application on the X80 chassis to handle email while scanning for spam and viruses. We ran two separate tests: one scanning email for viruses, and another scanning for spam and viruses.

InterScan Messaging Security Suite was loaded onto the Crossbeam APMs by Trend Micro staff, but was configured by Opus One. A separate management server, external to the Crossbeam chassis, was used for system and configuration management and for logging. When testing spam and virus handling, the application was configured to "tag and deliver" messages. This is somewhat unusual, since most enterprises and ISPs delete viruses and spam from their mail stream. However, we chose to have InterScan Messaging Security Suite deliver the mail both to put the worst case load on the system and to ensure that we could fully measure the message handling performance of the APM.

To measure performance, we used Spirent test equipment sending SMTP traffic into the InterScan Messaging Security Suite/Crossbeam system, and matching Spirent equipment at the other end to receive the messages from messaging security application. The Spirent Avalanche SMTP traffic generators were connected using 1 GigE interfaces, aggregated to a single GigE interface on the

Crossbeam X80 chassis. The SMTP traffic receivers were connected using a separate set of GigE interfaces, aggregated to a different GigE interface on the Crossbeam X80 chassis.

The Spirent SMTP sender was preloaded with 30 different email messages: 10 “normal” messages, 10 viruses, and 10 spam messages. The messages were selected at random from a live email stream a few days before the test was conducted. We configured the Spirent SMTP sender to deliver these messages to the Trend Micro/Crossbeam system in a ratio of 10 non-spam/89 spam/1 virus. This ratio represents a typical enterprise email load. These messages had sizes of between 4 KB and 108 KB.

The Trend Micro solution combines an open source MTA—Postfix—with Trend Micro’s own proprietary scanning technologies. Because Postfix can accept SMTP email faster than the spam and virus filters can scan the mail, we measured the performance of the InterScan Messaging Security Suite system in receiving, scanning, and delivering email while accepting a slightly higher level of email messages.

For example, we determined experimentally that a single APM has a performance capability for combined anti-spam and anti-virus scanning of between 60 and 65 messages per second. When a load of less than 60 messages per second is offered, the messaging security system will clear out messages as quickly as they come in and no queue will build up. When a load of 70 messages per second (for example), is offered, the queues begin to build up on the APM and the actual delivered mail rate is greater than 60 messages per second, but less than 70.

Using this example, we measured the message delivery performance of the InterScan Messaging Security Suite APM while a higher load than the delivery rate was being offered. For scanning for both spam and viruses, we offered a load of 65 messages per second per APM. When scanning only for viruses, we offered a load of 80 messages per second per APM.

Although the Spirent equipment was connected using Gigabit Ethernet networking, the relatively lower bandwidth requirement of email did not stress the network infrastructure. Even at highest load (nearly 800 messages/second), the total network bandwidth required to send the email was less than 300 Mbps. During our testing, we did not use any TLS/SSL encryption and we delivered exactly one email message to a single recipient per TCP connection.

To determine the performance of the Trend Micro/Crossbeam combination, we ran ten minute tests. The test had a ramp-up period of one minute, then steady transmission of email for five minutes. The end of the test was extended to give the InterScan Messaging Security Suite/Crossbeam system a chance to drain any queued messages. The message delivery rate was measured over a fixed three minute interval, two minutes into the test.

We also spot-checked delivery of messages to be sure that the InterScan Messaging Security Suite instance was still identifying viruses and spam in the offered load. No problems were found with messages slipping through under high loads.

Because our testing showed that the performance of the Crossbeam X80 chassis running InterScan Messaging Security Suite scales nearly linearly with the addition of APMs, we tested with 1, 2, 3, 4, 5, and 10 APMs. We believe that the numbers can be fairly and reliably extrapolated for APM counts between 6 and 9.

Results of Testing InterScan Messaging Security Suite

With a fully populated X80 chassis (ten APMs), our testing showed that InterScan Messaging Security Suite is capable of scanning for spam and viruses at speeds of 596 messages/second, and scanning for viruses at 754 messages/second. When configured with “N+1” redundancy, the chassis would be able to process 550 messages/second, scanning for both spam and viruses.

The performance numbers presented here should be considered as absolute maximum for unusual peak loads, and not as typical load limits. Because of the overhead involved in accepting and re-queueing messages when under high load, actual throughput is degraded when the offered load is much higher than capacity. For example, when a load of 150% (90 messages/second) is offered to an APM capable of handling 60 messages/second, the actual message delivery rate slows by 10%. As with InterScan Web Security Suite, a conservative sizing would call for continuous load levels of between 50% and 75% of the limits presented in this test.

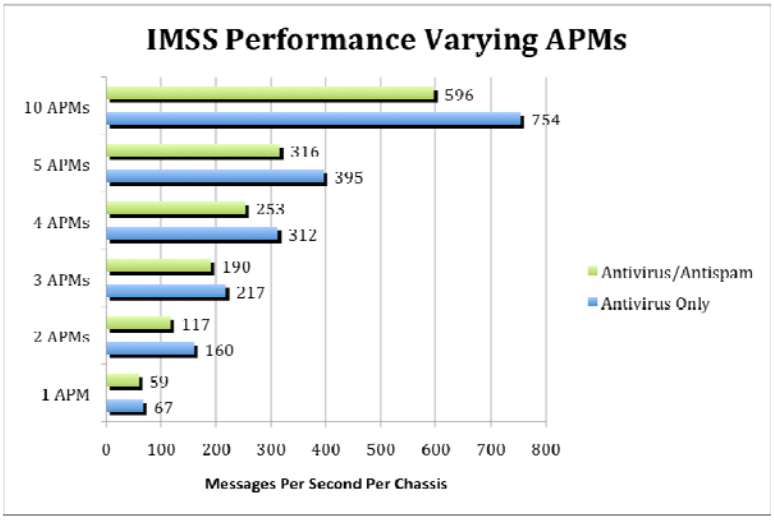

Figure 3: IMSS Performance Varying APMs

Anti-Spam Performance and Reputation Services

It is difficult to perform meaningful and repeatable benchmarks of email reputation services. However, Opus One's real-world testing has shown that reputation-based services are remarkably effective at identifying spam and reducing the load on anti-spam gateways.

Trend Micro offers an IP reputation service, Email Reputation Service (ERS). Their Email Reputation has two components, a reputation database that lists IP addresses that should always be refused email, and a dynamic service of IP addresses that are known to send spam, but which may also send non-spam mail. The intended behavior of anti-spam gateways is to refuse mail from IP addresses on the reputation database, and to offer a temporary refusal (4xx response in SMTP) for IP addresses identified through the dynamic service. The reputation database is intended to have a very low false positive rate, while the dynamic service will have a somewhat higher rate. However, because the addresses identified by the dynamic service should be given temporary refusals, the impact of an occasional false positive is that legitimate mail will delayed, but eventually would be accepted. In a recent, separate, Opus One test, the ERS reputation database had zero false positives in 10,000 messages, while the ERS dynamic service had 27 false positives.

Different anti-spam products use reputation services differently, but a common best practice is to refuse mail from systems that are listed on reputation service block lists such as those in the Trend Micro reputation database and dynamic service. This has the effect of dramatically increasing the potential performance of the anti-spam gateway, because between 50% and 80% of incoming spam can be blocked before it presents a load to the gateway.

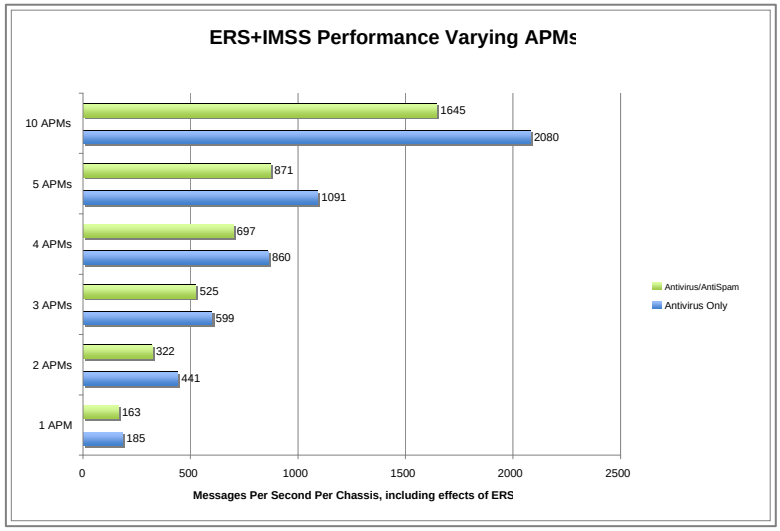

Figure 4: Predicted ERS + IMSS Performance Varying APM

In the most recent four months of testing, the average spam catch rate for the Trend Micro reputation database alone has been 47.7% and the spam catch rate of the Trend Micro dynamic service alone has been 28.4%, with a combined average catch rate of 76%. The average spam load, as a percentage of total messages, was 84%.

Thus, if an InterScan Messaging Security Suite/Crossbeam chassis were to use the reputation database and dynamic service to refuse suspected spam, it would be able to support a load 276% higher than the levels reported here, or approximately 1645 messages/second in a fully populated Crossbeam X80 chassis with 10 APMs.[1] Some vendors have used a factor of 500% or 1000% in their marketing literature for this type of testing, but we do not believe that these are credible results. A 500% increase in performance would require a mail stream that is 90% spam and a reputation service that is 90% effective; a 1000% increase would require 95% spam and 95% efficiency. These levels are not supported by our real-world research and testing.

Testing High Availability

One of the features of the Crossbeam X80 chassis is redundancy and high-availability support built into the underlying Crossbeam operating system. We performed some simple tests to validate that the X80 chassis and the InterScan Messaging Security Suite application fully support common high availability failure scenarios.

To test high availability, we configured a load of 550 messages/second across ten APMs running messaging security with anti-spam and anti-virus scanning enabled. This corresponds to an “N+1” redundancy configuration: we offered a load appropriate for nine APMs, to a chassis with ten APMs installed and operating. Our testbed had a single connection from the Spirent load generator to a dedicated Ethernet switch that had two connections to the Crossbeam chassis, each connected to a

[1] This is computed as 1/1-(spam load * reputation block rate).

separate Network Processing Module (NPM). A similar connection topology was used for the Spirent SMTP receiver: a single connection to a second dedicated switch, with dual connections from the switch to the Crossbeam X80 chassis. No special configuration of the switch was required to support these dual connections.

During the validation run, with ten APMs installed, we saw a throughput of 550 messages/second, equal to the offered load. This was expected because ten APMs can handle a load of 600 messages/second. We also observed that the load was spread evenly (or approximately) among all of the operating APMs.

We simulated one failure by unplugging one of the Ethernet cables attached to an active NPM port. This reproduced link loss, a failure that would occur if the connected switch or patch cable failed. Then, we simulated a second failure by abruptly removing one of the NPM cards installed in the Crossbeam chassis (leaving the second NPM with redundant connections in place). Although these failures did result in visible blips in the message flow, the final result was the same: 550 messages/second for the chassis. (The visible interruption was confirmed by an analysis of the second-by-second flows, showing a number of flows that were delayed during the HA event.)

Our third test simulated an application module failure by abruptly removing one of the APMs running the InterScan Messaging Security Suite application. When an APM or application failure occurs, the NPM is responsible for detecting the failure and redistributing traffic flows across healthy APMs. In this case, there was no drop in the message acceptance or delivery rate, with a final result of 550 messages/second across the test.

Conclusions

Opus One testing demonstrated that the capacity of the Crossbeam X80 chassis when teamed with Trend Micro InterScan Messaging Security Suite and InterScan Web Security Suite scales to very high levels as Application Processing Modules are added to the X80 chassis.

With a real-world HTTP scanning performance of 2.4 Gbps, and an email virus and spam scanning rate of 1645 messages per second, the combination of Crossbeam's X80 chassis and Trend Micro's Internet and email security applications provide the security services enterprises need at the speeds they need them.

Our testing of high availability services also proves the ability of the Crossbeam X80 chassis to survive failure scenarios without significantly affecting performance or the end-user experience.

About Opus One

Opus One is an information technology consultancy based in Tucson, Arizona. With 25 years of experience in the design and deployment of enterprise-class secure networks and email, Opus One provides unbiased and expert product evaluation services to enterprises on five continents.

Appendix I

Equipment Tested

IWSS v3.1 build 1027 with anti-virus and anti-spyware enabled was configured to scan all files submitted. Anti-virus engine version 8.500.1001 was loaded and no updates were allowed during the testing runs. Crossbeam hardware included the X80 chassis with two NPM-8200 modules, ten APM-8600 modules, and one CPM-8600 module. Crossbeam operating system was XOS v8.0.1.

IMSS v7.0 build 3167 with anti-spam engine version 5.0.1023 and anti-virus engine version 8.500.1001 was configured to tag-and-deliver all messages, including spam and viruses. Crossbeam hardware included the X80 chassis with two NPM-8200 modules, ten APM-8600 modules, and one CPM-8600 module. Crossbeam operating system was XOS v7.3. (At the time of testing, IMSS was not certified to run on XOS v8.)

Appendix II

X80 Chassis Configuration File for IWSS Test

```
#Do not remove after this line
# Last time the configuration was saved on Mon Apr 21 13:31:27.033634 2008 EDT
# Configuration generated by CLI on Mon Apr 21 13:33:38 2008
# CLI Version 8.0.0
#Do not remove above this line
#
configure
#
hostname IWSS_X80_A cp1
hostname IWSS_X80_B cp2
ip ftp
system-identifier 1
system-internal-network 1.1.0.0/16
operating-mode dual-np series-6
#
access-list 1001 permit ip source-ip 0.0.0.0 255.255.255.255 destination-ip 0.0.0.0 255.255.255.255
access-list 1002 permit ip source-ip 0.0.0.0 255.255.255.255 destination-ip 0.0.0.0 255.255.255.255
#
#
#
#
username admin privilege 15 gui-level administrator
#
#
alias wr 'copy running-config startup-config'
#
#
#
vap-group IWSS xslinux_v3
  vap-count 10
  max-load-count 10
  ap-list ap1 ap2 ap3 ap4 ap5 ap6 ap7 ap8 ap9 ap10
  load-balance-vap-list 1 2 3 4 5 6 7 8 9 10
  ip-flow-rule iwss_lbrule
    action load-balance
    activate
#
circuit mgmt circuit-id 1025
  device-name mgmt
  vap-group IWSS
    ip 8.8.8.11/24 8.8.8.255 increment-per-vap 8.8.8.20
circuit users circuit-id 1026
  device-name IMSS
  vap-group IWSS
    ip 172.16.1.1/24 172.16.1.255
circuit internet circuit-id 1027
  device-name internet
```


```
  vap-group IWSS
    ip 172.17.1.1/24 172.17.1.255
#
interface gigabitethernet 1/1
  logical mgmt
    circuit mgmt
interface 10gigabitethernet 1/10
interface 10gigabitethernet 1/12
  logical internet
    circuit internet
interface 10gigabitethernet 2/12
interface 10gigabitethernet 2/10
  logical users
    circuit users
#
redundancy-interface master 10gigabitethernet 1/12 backup 10gigabitethernet 2/11 mac-usage master
  failovermode preemption-off
redundancy-interface master 10gigabitethernet 2/12 backup 10gigabitethernet 1/11 mac-usage master
  failovermode preemption-off
#
management gigabitethernet 14/1
  ip-addr 8.8.8.10/24 8.8.8.255
  enable
  access-list 1001 input
  access-list 1002 output
#
management high-availability cp1
management high-availability cp2
#
management default-gateway 8.8.8.1
#
cp-action cp1 disk-error offline
cp-action cp2 disk-error offline
#
end
```

Appendix III

X80 Chassis Configuration File for IMSS Test

```
#Do not remove after this line
# Last time the configuration was saved on Mon Apr 21 13:31:27.033634 2008 EDT
# Configuration generated by CLI on Mon Apr 21 13:33:38 2008
# CLI Version 7.3.0
#Do not remove above this line
#
configure
#
hostname IMSS_X80_A cp1
hostname IMSS_X80_B cp2
ip ftp
system-identifier 1
system-internal-network 1.1.0.0/16
operating-mode dual-np series-2
#
access-list 1001 permit ip source-ip 0.0.0.0 255.255.255.255 destination-ip 0.0.0.0 255.255.255.255
access-list 1002 permit ip source-ip 0.0.0.0 255.255.255.255 destination-ip 0.0.0.0 255.255.255.255
#
#
#
#
username admin privilege 15 gui-level administrator
#
#
alias wr 'copy running-config startup-config'
#
#
#
vap-group IMSS xslinux_v3
  vap-count 10
  max-load-count 10
  ap-list ap1 ap2 ap3 ap4 ap5 ap6 ap7 ap8 ap9 ap10
  load-balance-vap-list 1 2 3 4 5 6 7 8 9 10
  ip-flow-rule imss_lbrule
    action load-balance
    activate
#
circuit mgmt circuit-id 1025
  device-name mgmt
  vap-group IMSS
    ip 8.8.8.11/24 8.8.8.255 increment-per-vap 8.8.8.20
circuit users circuit-id 1026
  device-name IMSS
  vap-group IMSS
    ip 172.16.1.1/24 172.16.1.255
circuit internet circuit-id 1027
  device-name internet
```


```
  vap-group IMSS
    ip 172.17.1.1/24 172.17.1.255
#
interface gigabitethernet 1/1
  logical mgmt
    circuit mgmt
interface gigabitethernet 1/4
interface gigabitethernet 1/6
  logical internet
    circuit internet
interface gigabitethernet 2/4
interface gigabitethernet 2/6
  logical users
    circuit users
#
redundancy-interface master gigabitethernet 1/6 backup gigabitethernet 2/4 mac-usage master
  failovermode preemption-off
redundancy-interface master gigabitethernet 2/6 backup gigabitethernet 1/4 mac-usage master
  failovermode preemption-off
#
management gigabitethernet 14/1
  ip-addr 8.8.8.10/24 8.8.8.255
  enable
  access-list 1001 input
  access-list 1002 output
#
management high-availability cp1
management high-availability cp2
#
management default-gateway 8.8.8.1
#
cp-action cp1 disk-error offline
cp-action cp2 disk-error offline
#
end
```