

WHERE TO GET HELP:

JTAC: [HTTP://WWW.JUNIPER.NET/SUPPORT](http://www.juniper.net/support) OR BY PHONE AT +1 888 341 JTAC OR 1-408-945-9500

J-NET COMMUNITY: [HTTPS://FORUMS.JUNIPER.NET/](https://forums.juniper.net/) THIS IS CUSTOMER FORUM WHERE YOU CAN ASK HOW-TO'S, SEARCH PREVIOUS QUESTIONS AND POST SOLUTIONS YOU WOULD LIKE TO SHARE. DX SPECIALISTS MONITOR THE SITE AND WILL ANSWER AS QUICKLY AS POSSIBLE.

COMMON FACTORY COMMANDS

FACTORY COMMANDS NORMALLY SHOULD NOT BE CHANGED BUT THE FOLLOWING ARE COMMON CHANGES THAT MAY BE REQUIRED. THEY ARE CLI ONLY. MOST OF THESE HAVE GLOBAL SETTING THAT CAN BE CUSTOMIZED AT THE CLUSTER LAYER. IF CLUSTER IS LISTED IT IS CUSTOMIZABLE. DOUBLE UNDERLINE> IS THE DEFAULT SETTING

```
set server factory sc <even number >=0, 5>
set cluster <name> factory a fcl <enabled|disabled>
set cluster <name> factory kac <enabled|disabled>
set cluster <name> factory kat <enabled|disabled>
set cluster <name> factory h w <enabled|disabled>
set cluster <name> factory h v <enabled|disabled>
set cluster <name> factory h ibh <0|1|2>
0= CLOSE CONN ON BAD HEADER
1= ALLOW BAD HEADERS; PASS THEM ON
2= IGNORE HEADERS BUT DO NOT FORWARD
```

New in 5.2 Cluster compression is in the WebUI. Server-wide is CLI only.

```
set cluster <name> compression msoffice <enabled|disabled>
set cluster <name> compression cmt 1 <MIME-type string>
set cluster <name> compression cmt 1 <MIME-type string>
set cluster <name> compression cmt 1 <MIME-type string>
set cluster <name> compression cmt <enabled|disabled>
set cluster <name> compression policy <0|1>
0= ALWAYS
1= NEVER
```

```
-SETS CONTENT CONNECTIONS; SOME APPS REQUIRE 0
-FORCES CONTENT LENGTH; TURNS OFF CHUNKED-MODE
-TURNS KEEP-ALIVE WITH CLIENTS ON/OFF
-TURNS KEEP-ALIVE WITH TARGETS ON/OFF
-TURNS "WARNING" HEADER ON/OFF
-TURNS "VIA" HEADER ON/OFF
-CHANGES HOW DX HANDLES BAD HTTP HEADERS
```

```
-TURNS COMPRESSION FOR OFFICE DOCS ON/OFF
-CUSTOMIZE UP TO 3 CUSTOM MIME-TYPES FOR COMPRESSION. FOR EXAMPLE, "TEXT/
JAVASCRIPT" IS NOT CORRECT BUT IT IS OFTEN MISLABELED ON SERVERS, SO DX DOES NOT
COMPRESS IT BY DEFAULT
-TURNS COMPRESSION FOR THE CLUSTER ON/OFF
EASY WAY TO TEST IF COMPRESSION IS BREAKING AN APP. OFTEN IT IS JUST ONE MIME
TYPE OR JUST ONE OBJECT. AN APPRULE CAN TURN IT OFF FOR THE OBJECT.
```

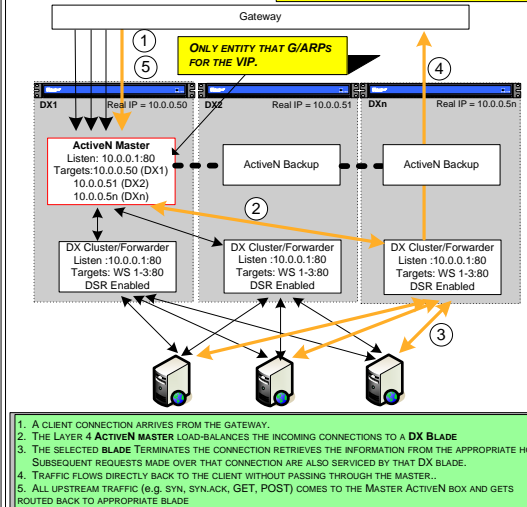
APPLICATION SPECIFIC CHANGES

MOST TIME DX DEFAULTS WORK JUST FINE. THERE ARE SOME APPS THAT MAY REQUIRE A FEW TWEAKS. THIS IS BY NO MEANS AN EXHAUSTIVE LIST.

APPLICATION	CHANGES OR THINGS TO LOOK FOR
ActiveX	SOMETIMES DOES NOT SUPPORT CHUNKED MODE, SET CLUSTER <NAME> A FCL ENABLED
BEA WebLogic v6.1+	1. MAY NEED STANDING CONNECTION SET TO 0 2. FOR IP LOGGING: -SET CLUSTER CUSTOMLOGHEADER TO WL-Proxy-Client-IP -On WebLogic 6.1+ admin console set the WebLogicPlugin to "Enabled" 2. TO INCREASE PERFORMANCE, INCREASE THE WEBLOGIC READ TIMEOUT VALUE (http://www.weblogic.com/docs51/admin/docs/properties.html) Set the client client timeout weblogic.login.readTimeoutMills=integer weblogic.login.readTimeoutMillsSSL=integer The default values are 5000 ms, with DX it can easily be set to 50000 ms
OUTLOOK Web Access	-ENABLE OWA IN THE CLUSTER. -FOR HTTPS TO HTTP CONVERSION, SEE APPRULE EXAMPLE ON PAGE 4.
MICROSOFT SHAREPOINT	-ENABLE OWA IN THE CLUSTER. -WITH XP AND THE LATEST VERSION OF SHAREPOINT, NOT ALL COMMUNICATION IS ALWAYS PORT 80 OR 443. THEY MAY USE THE FOLLOWING PORTS AS WELL. TCP PORT 445 FOR SMB TCP PORT 137 FOR NBNS UDP PORT 139 FOR NBSS. -SO 3 SLBs MAY BE REQUIRED.
NTLM	1. SET CLUSTER CONNBNB ENABLED 2. NTLM CHECKS THE DOMAIN OF THE REQUEST AND REQUESTER. -FOR TESTING: THE HOSTS FILE MAY NEED BE CHANGED TO MATCH THE SAME FQDN AS THE SITE OR DNS SHOULD BE UPDATED TO POINT TO THE DX VIP.
BLACKBOARD NOVELL NetStorage ENDECA	MOST LIKELY NEED - SET SERVER FACTORY SC 0

ActiveN Traffic Flow

NOTE: ALL TRAFFIC COMING FROM THE CLIENT GOES TO THE ACTIVE-N MASTER



1. A CLIENT CONNECTION ARRIVES FROM THE GATEWAY.
2. THE LAYER 4 ACTIVE-N MASTER LOAD-BALANCES THE INCOMING CONNECTIONS TO A DX BLADE
3. THE SELECTED BLADE TERMINATES THE CONNECTION RETRIEVES THE INFORMATION FROM THE APPROPRIATE HOST. SUBSEQUENT REQUESTS MADE OVER THAT CONNECTION ARE ALSO SERVICED BY THAT DX BLADE.
4. TRAFFIC FLOWS DIRECTLY BACK TO THE CLIENT WITHOUT PASSING THROUGH THE MASTER.
5. ALL UPSTREAM TRAFFIC (E.G. SYN, SYNACK, GET, POST) COMES TO THE MASTER ACTIVE-N BOX AND GETS ROUTED BACK TO APPROPRIATE BLADE

DX MULTIPLEXING & TCP OFFLOAD

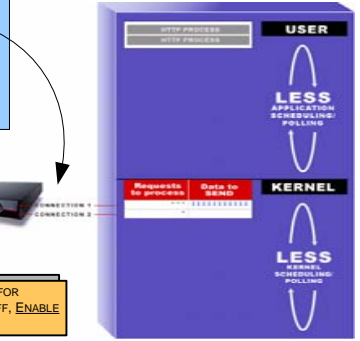
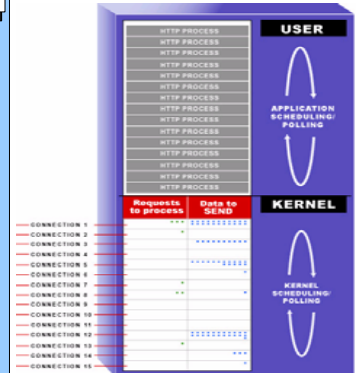
- HTTP/S RUNS OVER TCP. HANDLING THE BURDEN OF TCP FOR THE WEBSERVER IS ONE OF THE GREATEST BENEFITS DX PROVIDES
- EVERY BROWSER WINDOW OPENS BETWEEN 2-16 TCP CONNECTIONS TO THE SERVER (IE AND FIREFOX BOTH DEFAULT TO 2)
- DX MULTIPLEXES THESE CONNECTIONS SO THE WEB SERVER ONLY HAS A FEW HIGH SPEED, LOW LATENCY CONNECTIONS
- ON THE WAN, WEBSERVER CONNECTIONS AND PROCESSES ARE HIGHLY UNDER-UTILIZED. MANAGING THE CONNECTIONS AND THE SCHEDULING DRAMATICALLY REDUCES THE SERVER CAPACITY

DX WILL OFFLOAD CONNECTIONS UP TO SEVERAL THOUSAND TO ONE. REAL WORLD PUBLIC-SITES HAVE UP TO 1500+:1 RATIOS.

DX WILL NOT MULTIPLEX FOR THE SAKE OF MULTIPLEXING. IF MORE CONNECTIONS ARE NEEDED TO THE SERVER THEY WILL BE OPENED.



NOTE: SOME PROTOCOLS LIKE NTLM DO NOT ALLOW FOR MULTIPLEXING. IF MULTIPLEXING NEEDS TO BE SHUT OFF, ENABLE CONNECTION BINDING IN THE CLUSTER.



CLIENT IP ADDRESS VISIBILITY

DX IS A FULL PROXY IN CLUSTER MODE AND BY DEFAULT DOES FULL NAT IN SLB SO THE BACK END SERVERS WILL NOT SEE THE END-USER'S IP ADDRESS.

CLUSTER IP ADDRESS FORWARDING

DX CAN FORWARD CLIENT IP ADDRESSES IN AN HTTP HEADER. MOST REQUESTS FOR IP CAN BE SATISFIED WITH THIS METHOD. STARTING WITH 5.1 THIS HEADER IS ON A CLUSTER BY CLUSTER BASIS.

```
set cluster <name> customiplogheader <anything you to name it>
```

APACHE:
In httpd.conf change %h to %(anything_you_to_name_it)

IIS
THERE IS AN ISAPI FILTER FOR IIS SERVERS CALLED RLLOG.DLL AVAILABLE FROM SUPPORT, J-NET THAT WILL ALLOW IIS SERVERS TO LOG CLIENT IP ADDRESS IN THEIR ACCESS LOGS.

For IIS only you need to use:

```
set cluster <name> customiplogheader rliclientipaddr
```

FOR OTHER WEBSERVERS OR DEVICES CHECK THE DX ADMIN GUIDE

CLUSTER IP TRANSPARENCY

IF THE WEBSERVER LOOKS INTO THE IP STACK FOR IP ADDRESS YOU MAY NEED TO ENABLE CLUSTER TRANSPARENCY:

```
set cluster <name> transparency enabled
```

NOTE: YOU LOSE MULTIPLEXING BECAUSE CONNECTION BINDING WILL BE SET FOR THE CLUSTER
NOTE: YOU MUST SET THE DX AS THE DEFAULT GATEWAY OF THE SERVERS IN QUESTION

SLB HALF-NAT

IF THE BACK-END SERVER LOOKS INTO THE IP STACK FOR IP ADDRESS YOU WILL NEED TO SET HALF-NAT IN THE SLB GROUP

```
set slb group <name> nat half OR IN THE WEBUI SELECT HALF-NAT
```

NOTE: YOU MUST SET THE DX AS THE DEFAULT GATEWAY OF THE SERVERS IN QUESTION

COMMAND LINE ONLY:

```
CONFIG SYNC (DX 5.1 ADMIN GUIDE PAGE 136)
SNAT (DX 5.1 ADMIN GUIDE PAGE 154)
FLOATING VIP (DX 5.1 ADMIN GUIDE PAGE 156)
ADDING CACHE (DX 5.1 ADMIN GUIDE PAGE 271)
VLAN TAGGING (DX 5.1 ADMIN GUIDE PAGE 160)
STATIC ROUTE (DX 5.1 CLI GUIDE PAGE 53)
MULTIMETTING THE NICS (DX 5.1 CLI GUIDE PAGE 49)
FACTORY SETTINGS (CONTACT JTAC OR YOUR SE)
LICENSING (DX 5.1 ADMIN GUIDE PAGE 123)
RUNNING 'TOPDUMP' (SET UP AVAILABLE IN WEBUI)
RUNNING 'TSDUMP' (SET UP AVAILABLE IN WEBUI)
RUNNING 'INSTALL' (SET UP AVAILABLE IN WEBUI)
```

A MAJORITY OF FUNCTIONALITY IS IN THE WEBUI AND WITH EACH RELEASE MORE WEBUI FUNCTIONALITY IS ADDED. AS OF 5.2 THESE TASKS ARE CLI ONLY

CONFIG SYNCHRONIZATION:

THESE ARE THE BASIC STEPS NEEDED TO SETUP CONFIG SYNC. YOU MAY NEED TO USE AN OVERRIDE FILE IF YOU DO NOT WANT CERTAIN SETTINGS SYNCED (ADMIN GUIDE PAGE 136)

BASIC CONFIG

```
dx% add sync group <name>
dx% add sync group <name> member <IP address1>
dx% add sync group <name> member <IP addressN>
dx% set sync group <name> member <IP address1> password
<enter password twice>
dx% set sync group <name> member <IP addressN> password
<enter password twice>
dx% sync group <name>
```

WHAT IS NOT SYNCED:
HOSTNAME
ALL ETHER SETTINGS
DEFAULT ROUTE
ADMIN VIP AND INTERFACE SETTINGS
ADMIN SOAP SETTINGS
FAILOVER STATIC PEERS

IN ANY ACTIVE-N OR FAILOVER GROUP YOU ONLY NEED TO CONFIGURE ONE BOX THEN YOU CAN PUSH CONFIG CHANGES TO ALL BOXES. ONCE CONFIG IS ON ALL BOXES YOU CAN MAKE CHANGES ON ANY BOX. HOWEVER MAKING CHANGES ON THE ACTIVE ARE RECOMMENDED TO KEEP THE BOXES FROM FAILING OVER

QUICK REFERENCE APPRULE MATRIX

RULE TYPE/ SYNTAX MATRIX

RULE TYPE

FOR REQUEST SENTRY RULES: WITH THE EXCEPTION OF THE LOG ACTION, ONLY ONE ACTION MAY BE PRESENT IN A SINGLE RULE.

	VARIABLES										
RS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
RTH	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
PTH	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
PTC	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

	TEST OPERATORS															
RS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
RTH	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
PTH	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
PTC	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

	ACTIONS																			
RS	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
RTH	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
PTH	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
PTC	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

VARIABLE/TEST OPERATOR RELATIONSHIPS

THIS TABLE LISTS THE LEGAL RELATIONSHIPS BETWEEN THE VARIABLES AND TEST OPERATORS. NOTE THAT JUST BECAUSE A RELATIONSHIP EXISTS, DOES NOT MEAN THAT IT CAN BE USED FOR EVERY RULE. FOR EXAMPLE, THE URL VARIABLE CAN BE USED WITH THE VARIOUS LENGTH OPERATORS, BUT ONLY FOR REQUEST SENTRY RULES (SEE THE RULE TYPE/SYNTAX MATRIX ABOVE FOR WHICH RULES USE WHICH VARIABLES AND TEST OPERATORS).

VARIABLES	(NOT)_EXISTS	(C)_NOT_EQUALS	(C)_NOT_CONTAINS	(C)_NOT_STARTS_WITH	(C)_NOT_ENDS_WITH	LENGTH_(GREATER/LESS)_THAN	LENGTH_(NOT)_EQUALS
URL **ACTUALLY URI**						✓	
QUERY_STRING	✓	✓	✓	✓	✓		✓
HTTP_METHOD							
SRC_IP (SIP)	✓	✓	✓	✓	✓		✓
SRC_IP1; SRC_IP2; SRC_IP3; SRC_IP4							
SSL_VERSION							✓
SSL_CIPHER_BITS							✓
SSL_CIPHERSUITE		✓	✓	✓	✓		
HTTP_REQUEST_VERSION							
REQUEST_HEADER	✓	✓	✓	✓	✓		✓
ANY_REQUEST_HEADER	✓	✓	✓	✓	✓		✓
REQUEST_COOKIE							
ANY_REQUEST_COOKIE	✓	✓	✓	✓	✓		✓
REPLY_HEADER	✓	✓	✓	✓	✓		✓
HTTP_REPLY_CODE							
HTTP_REPLY_VERSION							
REPLY_COOKIE							
CONTENT	✓	✓	✓	✓	✓		✓

COPYRIGHT © 2006 BY JUNIPER NETWORKS. ALL RIGHTS RESERVED. NO PART OF THIS PUBLICATION MAY BE REPRODUCED, STORED IN A RETRIEVAL SYSTEM OR TRANSMITTED IN ANY FORM OR BY ANY MEANS, ELECTRONIC, MECHANICAL, PHOTOCOPYING, RECORDING, SCANNING OR OTHERWISE, WITHOUT THE PRIOR WRITTEN CONSENT OF JUNIPER NETWORKS.

GENERAL RULE SYNTAX

```
<RULE_TYPE>: <TEST_CONDITION> [...AND <TEST_CONDITION>] THEN
<ACTION_STATEMENT> [...AND <ACTION_STATEMENT>] [AND CONTINUE]
```

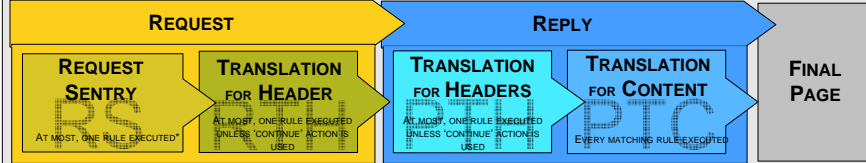
WHERE
<RULE_TYPE> IS A VALID RULE TYPE (RS, RTH, PTH, PTC)
<TEST_CONDITION> IS A VALID TEST CONDITION OF THE FORM
<VARIABLE> <OPERATOR> ["<ARGUMENT>"]
<ACTION_STATEMENT> IS A VALID ACTION STATEMENT OF THE FORM
<ACTION> ["<ARGUMENT>"]

MULTIPLE TEST CONDITIONS AND MULTIPLE ACTION STATEMENTS MAY BE JOINED TOGETHER IN A SINGLE RULE USING THE AND KEYWORD.

USING 'AND CONTINUE' AT THE END OF RS (ONLY LOGGING RULES), RTH & PTH RULES ALLOW PROCESSING OF MULTIPLE RULES IN ORDER. IT CANNOT BE USED WITH I/O ACTIONS LIKE ROUTE_REQUEST OR FORWARD.

ALL USER-SUPPLIED ARGUMENTS MUST BE ENCLOSED IN DOUBLE QUOTES.

RULE TYPES AND EXECUTION ORDER



SUPPORTED HEADERS (CASE-SENSITIVE)	Accept	Accept-Charset	Accept-Encoding	Accept-Language	Accept-Ranges	Age	Allow
Accept	Accept-Charset	Accept-Encoding	Accept-Language	Accept-Ranges	Age	Allow	Connection
Allow-Rename	Apply-To-Redirect-Ref	Authorization	Content-Content-Language	Brief	Cache-Control	Call-Back	Content-Range
Content-Base	Content-Encoding	Content-Type	Cookie	Content-Length	Content-Location	Content-MD5	Depth
Destination	Edge-Control	Host	Keep-Alive	ETag	Date	Expires	FRONT-END-HTTPS
Notification-Delay	Label	Notification-Type	Proxy-Authenticate	If-Modified-Since	If-None-Match	If-Range	If-Unmodified-Since
Proxy-Authenticate	Notification-Type	Proxy-Authorization	Retry-After Server	Location	Lock-Token	Position	Max-Forwards
Subscription-Lifetime	Set-Cookie	Set-Cookie2	TE	Overwrite	Range	Redirect-Ref	Referer
Transfer-Encoding	Upgrade	User-Agent	WWW-Authenticate	Public	Status-URI	Trailer	TransactionID
X-CIMS-Cache-Control	X-Powered-By	X-Rin-Effective-Len		SSL Client Cipher	Transaction	Warning	WL-Proxy-SSL

LEGAL RELATIONSHIPS BETWEEN PREPEND, APPEND, REPLACE ACTIONS WITH VARIABLES AND TEST OPERATORS

RULE TYPE	VARIABLES				TEST OPERATORS			
	URL	QUERY_STRING	REQUEST_HEADER	REPLY_HEADER	CONTENT	(C)_CONTAINS	(C)_STARTS_WITH	(C)_ENDS_WITH
REQUEST SENTRY (RS)								
REQUEST TRANSLATOR HEADER (RTH)	✓	✓	✓			✓	✓	✓
PAGE TRANSLATOR HEADER (PTH)				✓		✓	✓	✓
PAGE TRANSLATOR CONTENT (PTC)					✓	✓		

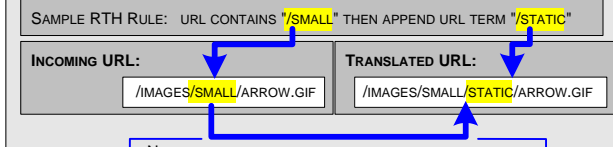
ESCAPE CHARACTERS & USING THE WILDCARD *

THE CONTENT VARIABLE (PTC ONLY) CAN CONTAIN A SINGLE WILDCARD "*" CHARACTER WHICH WILL MATCH UP TO 26 ARBITRARY CHARACTERS. THE SEARCH TERM MAY NOT START OR END WITH THE WILDCARD. IN ADDITION, SEVERAL ESCAPED CHARACTERS ARE ALSO AVAILABLE:

\\	NEWLINE
\/	CARRIAGE RETURN
\"	DOUBLE QUOTE
\/	ASTERISK
\/	BACKSLASH

EXAMPLE:
 SEARCH STRINGS: \\"*FIND\"ME!
 \\"*FIND\"ME2!
 CONTENT STRING: \"\\/\"*FIND\"ME\"!\\!\"*
↑ WILDCARD

STRING MATCHING WITH TERM KEYWORD



NOTE THAT BECAUSE THE TERM KEYWORD IS USED, THE STRING "/>

IF MULTIPLE INSTANCES OF THE VARIABLE BEING ACTED UPON EXISTS IN THE RULE, THEN THE PREPEND, APPEND, OR REPLACE ACTION WILL OCCUR AGAINST THE FIRST INSTANCE OF THAT VARIABLE.

SAMPLE RTH RULE:
 URL SW "/>

THE STRING "/>

QUICK REFERENCE

TIPS FOR WRITING RULES:

- ✓ PLACE RULES THAT GET HIT MORE OFTEN NEAR THE TOP OF THE RULE LIST.
- ✓ USE CASE-SENSITIVE SEARCHES WHERE POSSIBLE.
- ✓ PREFER OPERATORS LIKE **STARTS_WITH** AND **ENDS_WITH** OVER THE **CONTAINS** OPERATOR, BUT USE THE **CONTAINS** OPERATOR IF IT MEANS FEWER INDIVIDUAL RULES.
- ✓ WHEN USING THE **CONTAINS** OPERATOR, USE THE LONGEST POSSIBLE STRING TO ENABLE A MATCH, BUT WHEN USING **STARTS_WITH** AND **ENDS_WITH**, USE THE SHORTEST SEARCH STRING.
- ✓ AVOID THE USE OF THE **!** WILDCARD WHERE POSSIBLE.
- ✓ REDUCE RULE COUNT BY USING THE **AND** KEYWORD TO JOIN TEST CONDITIONS AND ACTIONS WHERE POSSIBLE.

APPRULE EXAMPLES

THESE ARE BY NO MEANS A LIST OF ALL EXAMPLES. NEW APPRULE USE CASES COME UP EVERY DAY. IF YOU DON'T SEE YOUR SPECIFIC APPLICATION OR NEED HERE, YOU MAY WANT TO TRY [HTTP://COMMUNITIES.JUNIPER.NET/DCA](http://communities.juniper.net/dca) TO SEE IF NEW RULES HAVE BEEN POSTED. YOU CAN ASK THE COMMUNITY (THIS WILL HELP EVERYONE) OR YOU CAN CONTACT YOUR SE OR JUNIPER SUPPORT AT [HTTP://WWW.JUNIPER.NET/SUPPORT](http://www.juniper.net/support). SOME OF THESE RULES ARE JUST A STARTING POINT TO GIVE YOU AN IDEA OF WHAT IS POSSIBLE YOU MAY NEED TO CUSTOMIZE THE RULE TO FIT YOUR NEEDS.

USE CASE AND RULESET

REWRITE HTTP APPLICATION TO HTTPS

BASIC WEB APP

PTH: reply_header "Location" contains "http://www.site.com" then
replace reply_header "Location" term "https://www.site.com" and continue

PTC: content contains "http://www.site.com" then
replace content term "https://www.site.com"

OPTIONAL >>> THE FOLLOWING MAY BE NEEDED FOR SPECIFIC APPS:

Outlook Web Access HTTP to HTTPS

RTH: request_header "Host" eq "webmail.site.com" then
insert_request_header "FRONT-END-HTTPS" "ON"

PeopleSoft HTTP to HTTPS

RTH: request_header "Referer" starts_with "https://www" then
replace request_header "Referer" term "http://www" and continue

RTH: request_cookie "ExpirePage" contains "https:" then
replace request_cookie "ExpirePage" term "http:" and continue

RTH: request_cookie "PS_LOGINLIST" contains "https:" then
replace request_cookie "PS_LOGINLIST" term "http:" and continue

RTH: request_cookie "PS_TOKENEXPIRE" contains "https%3a" then
replace request_cookie "PS_TOKENEXPIRE" term "http%3a" and continue

RTH: query_string contains "https%3a" then
replace query_string term "http%3a" and continue

PTH: reply_header "Referer" starts_with "http://www" then
replace reply_header "Referer" term "https://www" and continue

PTH: reply_cookie "ExpirePage" contains "http:" then
replace reply_cookie "ExpirePage" term "https:" and continue

PTH: reply_cookie "PS_LOGINLIST" contains "http:" then
replace reply_cookie "PS_LOGINLIST" term "https:" and continue

PTH: reply_cookie "PS_TOKENEXPIRE" contains "http%3a" then
replace reply_cookie "PS_TOKENEXPIRE" term "https%3a" and continue

PTC: content contains "http%3a%2f%2fwww.site.com" then
replace content term "https%3a%2f%2fwww.site.com"

NOTES

CHANGES 302 REPLIES TO REFERENCE THE HTTPS PORT INSTEAD OF HTTP PORT THAT THE TARGET WEBSERVER THINKS IT'S TALKING ON SO THE END USER HITS THE DX ON HTTPS.

CHANGES ALL HARDCODED LINKS TO SSL. RELATIVE LINKS WITHIN THE PAGE DON'T NEED TO BE CHANGED.

INSERTS THE FRONT-END-HTTPS HEADER TO ALL REQUESTS. OWA REQUIRES THIS HEADER SO YOU DON'T HAVE TO MODIFY ALL LINKS AND HEADERS.

--THESE ARE JUST A STARTING POINT FOR CONVERTING HTTP TO HTTPS FOR PEOPLESOFT ENTERPRISE. YOU MAY NEED TO GET A BIT MORE SPECIFIC WITH YOUR LINKS SO INSTEAD OF JUST LOOKING FOR "http://" YOU MAY WANT TO LOOK FOR HTTP://INSTANCE.SITE.COM"

--YOU MAY NEED TO DOUBLE UP RULES BECAUSE AS SOON AS A RULE HITS IT STOPS PROCESSING (IN THE CASE OF "AND CONTINUE" IT GOES TO THE NEXT RULE). FOR INSTANCE IF YOU ARE LOOKING FOR "https%3a" IN THE QUERY STRING THERE MAY BE MORE THAN ONE INSTANCE OF "https%3a" IN THE QUERY STRING, YOU WILL NEED THE SAME RULE 3 TIMES:

?NEXT_URL=https%3a%2f%2fwww.site1.com&LOGOUT_URL=https%3a%2f%2fwww.site2.com&HOME_URL=https%3a%2f%2fwww.site3.com

RTH: query_string contains "https%3a" then
replace query_string term "http%3a" and continue

RTH: query_string contains "https%3a" then
replace query_string term "http%3a" and continue

RTH: query_string contains "https%3a" then
replace query_string term "http%3a" and continue

--UNICODE NEEDS TO BE SPELLED OUT SPECIFICALLY WITH "%&" AND HEX VALUES IF IT COMES FROM THE BROWSER OR SERVER THAT WAY.

FOR EXAMPLE:
HTTP:// == HTTP%3A%2F%2F

NOTICE THE USE OF THE ESCAPE BACKSLASH. MOST HEADERS DO NOT HAVE QUOTES IN THEM, BUT IN ORDER TO GET THEM YOU NEED TO ADD \"

SIEBEL IS A GOOD EXAMPLE OF AN APP THAT MAY USE 2 DIFFERENT HEADERS TO GET THE SAME REDIRECT ACTION. YOU MAY NEED BOTH RULES IF YOU AREN'T GETTING REDIRECTED CORRECTLY. THIS IS USUALLY ONLY AN ISSUE IF YOU ARE TRYING TO CHANGE THE HOSTNAME OF THE APP OR CONVERTING FROM HTTP TO HTTPS. "CONTENT-LOCATION" ALLOWS FOR RELATIVE REDIRECTS. "LOCATION" REQUIRES AN ABSOLUTE URL.

-ROUTE REQUEST ALLOWS FOR TRUE LAYER 7 LOAD BALANCING.

-THE TARGET HOSTS NEED TO BE PART OF THE CLUSTER. DON'T FORGET TO INCLUDE THE IP AND PORT.

-HOSTS ARE LOAD BALANCED WITH THE DX FEWEST OUTSTANDING REQUESTS ALGORITHM

-ROUTE_REQUEST OVERRIDES STICKY

INSERT P3P HEADER TO ALL REQUESTS

PTH: url starts_with "/" then
insert_reply_header "P3P" "CP=HAO FOR SKE CIO ZPRA"

MODIFY REDIRECTS FOR SIEBEL WEB

PTH: reply_header "Location" contains "http://siebel.site.com" then
replace reply_header "Location" term "https://dsiebel.site.com"

PTH: reply_header "Content-Location" contains "http://siebel.site.com" then
replace reply_header "Content-Location" term "https://dsiebel.site.com"

ROUTE REQUEST EXAMPLES

RTH: url starts_with "/images" then
route_request target_host "2.2.2.10:80" "2.2.2.11:80"

RTH: request_header "Host" equals "www.site1.com" then
request_cookie "rsticky" not_exists then
route_request target_host "2.1.1.10:80" "2.1.1.11:80"

RTH: request_header "Host" equals "www.site2.com" and
request_cookie "rsticky" not_exists then
route_request target_host "2.1.1.12:80" "2.1.1.13:80"

RTH: request_cookie "JSESSIONID02" exists then
route_request target_host "10.200.6.2:80"

RTH: request_cookie "JSESSIONID03" exists then
route_request target_host "10.200.6.3:80"

RTH: request_cookie "JSESSIONID04" exists then
route_request target_host "10.200.6.4:80"

APPRULE EXAMPLES (CONTINUED)

THESE ARE BY NO MEANS A LIST OF ALL EXAMPLES. NEW APPRULE USE CASES COME UP EVERY DAY. IF YOU DON'T SEE YOUR SPECIFIC APPLICATION OR NEED HERE, YOU MAY WANT TO TRY [HTTP://COMMUNITIES.JUNIPER.NET/DCA](http://communities.juniper.net/dca) TO SEE IF NEW RULES HAVE BEEN POSTED. YOU CAN ASK THE COMMUNITY (THIS WILL HELP EVERYONE) OR YOU CAN CONTACT YOUR SE OR JUNIPER SUPPORT AT [HTTP://WWW.JUNIPER.NET/SUPPORT](http://www.juniper.net/support). SOME OF THESE RULES ARE JUST A STARTING POINT TO GIVE YOU AN IDEA OF CHANGES YOU MAY NEED TO CUSTOMIZE.

USE CASE AND RULESET

CACHING RULES

PTH: http_reply_code equals "200" and
reply_header "Content-Type" contains "image" then
cache "604800"

PTH: http_reply_code equals "200" and
reply_header "Content-Type" contains "javascript" then
cache "86400"

PTH: http_reply_code equals "200" and
reply_header "Content-Type" contains "css" then
cache "86400"

REDIRECTION RULES

RS: url equals "/" then
redirect "https://" "login.html"

Rs: request_header "Referer" not_contains "www.mysite.com" then
redirect "http://www.mysite.com" "donstae.html"

APP REQUIRES HOSTNAME AND YOU CANNOT CHANGE HOSTS FILE

RTH: request_header "Host" equals "10.10.1.2" then
update_request_header "Host" "www.site.com"

PTH: reply_header "Location" contains "www.site.com" then
update_reply_header "Location" term "10.10.1.2"

PTC: content contains "www.site.com" then
replace content term "10.10.1.2"

TURN ON COMPRESSION FOR NORTON USERS

RTH: request_header "-----" exists then
insert_request_header "Accept-Encoding"

BASIC HIGH AVAILABILITY RULES

REQUEST_RETRY

PTH: http_reply_code starts_with "5" then
retry_request same "3" and log

PTH: http_reply_code equals "404" then
retry_request nosame "3" and log

PTC: content ci_contains "sj error" then
retry_request same "3" and log

TURNING OFF COMPRESSION FOR SPECIFIC OBJECTS

RTH: url ends_with "/agent.dll" then
delete_request_header "Accept-Encoding"

RTH: request_header "User-Agent" contains "IE 5" and
url ends_with ".pdf" then
delete_request_header "Accept-Encoding"

DROP TO FORWARDER

RTH: url starts_with "/dana/" then forward

PTH: reply_header "Server" contains "FoaAppServer" then forward

NOTES

DEPLOYING A NEW CACHE (FROM THE CLI):
add cache [cache_name]
set cluster <cluster_name> cache <cache_name>
set cluster <cluster_name> cache <cache_name> enabled
##OPTIONAL###
set cache <cache_name> max_objects <1-65535>
set cache <cache_name> size <1048576-[10485600|32xx]-83860800(36xx)>

NOTE: CACHING IS BASED IN APPRULES SO DON'T FORGET TO ENABLE THE APPRULE FOR THE CLUSTER IN QUESTION. SERVICES >>>CLUSTER GROUPS>>>APPRULES>>> CHOOSE THE FILE AND CLICK ENABLED

APPRULE REDIRECTION PROVIDES MUCH MORE FLEXIBILITY THAN THE REDIRECTOR MODULE. IF YOU WANT ALL REQUESTS FROM PORT 80 TO BE REDIRECTED TO 443 USE A REDIRECTOR. IF YOU WANT TO CUSTOMIZE WHEN AND WHY YOU REDIRECT USE APPRULES.

THE HOST NAME SENT FROM THE END USER IS TAKEN INTO ACCOUNT. SO IN THE FIRST EXAMPLE ON THE LEFT, IF THE END USERS TYPED "WWW.SITE1.COM" THEY WILL BE REDIRECTED TO "HTTPS://WWW.SITE1.COM/LOGIN.HTML." IF THE USERS TYPE "WWW.SITE2.COM" IN THE BROWSER THEY WILL REDIRECT TO "HTTPS://WWW.SITE2.COM/LOGIN.HTML."

THE SECOND EXAMPLE WOULD HELP STOP PEOPLE FROM LINKING TO YOUR SITE ILLEGALLY BY REQUIRING THE REFERER HEADER TO MATCH YOUR SITE.

THIS RULE IS GOOD FOR TRIALS OR TESTS WHERE YOU CANNOT CHANGE THE HOSTS FILE ON MULTIPLE MACHINES. SOME APPLICATIONS REQUIRE A KNOWN HOSTNAME.

THE RULE CHANGES ALL REQUESTS TO THE VIP IP TO HAVE THE CORRECT HOST HEADER, THEN CHANGES ANY REDIRECTS FROM THE SERVER AS WELL AS HARDCODED LINKS TO THE CLUSTER IP ON THE WAY OUT TO THE END USER.

SOMETIMES NORTON ANTI-VIRUS TURNS OFF COMPRESSION FOR WEB BROWSERS BY REPLACING THE ACCEPT-ENCODING HEADER WITH TLDES, WHICH IN TURN, HURTS PERFORMANCE. TURN IT BACK ON WITH THIS RULE.

ERROR CODES SENT TO THE END USER ARE OFFICIALLY DOWN TIME AS SHORT LIVED AS THEY MAY BE. SOME ERROR CODES MAY EVEN GIVE AN ATTACKER SENSITIVE INFORMATION ABOUT THE WEBSERVER. REQUEST_RETRY KEEPS ERRORS FROM GOING TO THE END USER.

ON RARE OCCASIONS THERE ARE TIMES THAT BROWSER BUGS ARE DISCOVERED WITH COMPRESSION. ONCE YOU FIND THE CULPRIT, USE RULES LIKE THIS TO TURN OFF COMPRESSION FOR THE SMALLEST AMOUNT OF USERS OR PAGES POSSIBLE. YOU DON'T WANT TO HAVE TO TURN OFF COMPRESSION COMPLETELY.

NEW IN 5.2 - DX IS VERY STRICT WITH HTTP. GENERALLY IF AN APP BREAKS THE HTTP PROTOCOL THE CONNECTION WILL BE DROPPED. THERE ARE TIMES WHEN THIS NEEDS TO BE OVERRIDDEN. APPS LIKE THE SA (SAM AND NC) ARE GOOD EXAMPLES. THE SA COMPATIBILITY BUTTON ESSENTIALLY DOES THE FIRST EXAMPLE FOR YOU. THIS IS A GREAT TROUBLESHOOTING TOOL. FORWARD ESSENTIALLY TURNS THE CONNECTION INTO A TCP PROXY SO YOU WON'T NEED TO USE MAKE FORWARDER GROUP IF AN APP BREAKS THROUGH A DX CLUSTER. IT CANNOT BE FOLLOWED WITH "CONTINUE" AND ONCE IT RUNS, THE CONNECTION IS OUTSIDE OF A CLUSTER SO COMPRESSION, MULTIPLEXING, APPRULES NO LONGER APPLY

Notes: