	Cisco Router의 wccp와 SQUID		
문서번호: HINetworks-20171130-01		**버전:** 1.0	**Date:** 2017/11/30

1. 라우터에 wccp관련 설정하기

```
ip cef
ip wccp web-cache redirect-list 100
```
: web-cache는 80/TCP만. ACL 100에 정의된 트래픽을 캐시서버로 redirect시키라고 정의
```
ip wccp 70 redirect-list 150
```
: https(443/TCP)를 redirect시키기 위해서 dynamic service 70을 정의함. 70번호는 squid설정에서도 연관되어져야 함.

```
interface Ethernet0/2
 ip address 10.200.1.1 255.255.255.0
  …
 ip wccp web-cache redirect in
 ip wccp 70 redirect in
```
: Eth0/2인터페이스로 inbound되는 트래픽을 캐시서버로 redirect. 10.200.1.0/24네트워크의 노드들드에서 http, https연결이 캐시서버로 redirect되도록 설정.
```
  …

access-list 100 deny   ip host 10.100.1.100 any
access-list 100 permit ip any any
access-list 150 permit tcp any any eq 443
```

2. SQUID서버에 GRE터널 생성하기
   - SQUID서버가 누구하고 GRE터널을 맺어야 하는가? 라우터에서 show ip wccp했을 때 나오는 Router Identifier의 주소와 맺어야 한다고 함.

```
R1#show ip wccp
Global WCCP information:
    Router information:
        Router Identifier:                   192.168.10.151
        Protocol Version:                    2.0
```
   - SQUID서버에서 GRE터널 수동으로 생성하기

ip tunnel add wccp0 mode gre remote 192.168.10.151 local 10.100.1.100 dev ens3 ttl 255

: ip tunnel명령으로 GRE터널을 정의. wccp0가 터널인터페이스의 이름인데 이것은 임의로 지정하지만, 지정한 이름을 그 이후에 인터페이스명에는 동일하게 사용해야 함.
위의 명령으로 설정한 후에 ip tunnel명령을 입력해서 정의된 값 확인.

ip link set wccp0 up

: 생성된 wccp0인터페이스를 활성화 시킴. ifconfig -a명령으로 IP설정없이 wccp0가 up이 된 것을 확인함.

3. 리눅스 커널 파라미터 값 주의하기
   - ip_forward값 설정하기

리눅스는 한 개 이상의 NIC를 가지고 그 인터페이스간에 통신이 되도록 하려면(즉, 라우팅기능을 활성화 하려면) 커널의 ip_forward값을 1로 설정을 해주어야 함. SQUID서버에 물리 ens3인터페이스와 grep터널 wccp0인터페이스가 있고, 두 인터페이스간에 통신이 되어야하기 때문에 ip _forward값을 1로 설정하는 것이 필요함.

```
# sysctl -w net.ipv4.ip_forward=1
```

   - rp_filter값 disable하기

이 문제 때문에 많은 시간을 소비했는데 리눅스의 rp_filter기능은 reverse path를 체크하는 기능이라고 함. 즉, 리눅스가 패킷을 받았을 때 출발지 IP를 확인하는것인데 출발지 IP가 리눅스서버의 라우팅테이블에 있어야 패킷이 drop되지 않는다고 함. redirect되는 서브넷이 많은 경우에 리눅스 서버에 일일히 라우팅을 추가하는 것은 좋은 방법이 아닌 것 같으므로 모든 네트워크 인터페이스에 대해서 rp_filter값을 disable해서 체크하지 않도록 설정함.

```
# sysctl -w net.ipv4.conf.all.rp_filter=0
# sysctl -w net.ipv4.conf.default.rp_filter=0
# sysctl -w net.ipv4.conf.ens3.rp_filter=0
# sysctl -w net.ipv4.conf.gre0.rp_filter=0
# sysctl -w net.ipv4.conf.gretap0.rp_filter=0
# sysctl -w net.ipv4.conf.wccp0.rp_filter=0
```

4. SQUID 소스로 컴파일하기

우분투 리눅스에서 squid를 apt명령으로 설치해서 시험을 했지만, http 트래픽에 대해서만 캐시하도록 컴파일된것이어서 http트래픽까지 시험하기 위해서 소스 컴파일을 수행함.

참고문서:
https://www.chasewright.com/install-squid-from-source-on-ubuntu-16-04/

configure를 실행할 때 아래의 옵션으로 config를 수행했음.

```
#./configure '--build=x86_64-linux-gnu' '--prefix=/usr' '--includedir=${prefix}/include' '--mandir=${prefix}/share/man' '--infodir=${prefix}/share/info' '--sysconfdir=/etc' '--localstatedir=/var' '--libexecdir=${prefix}/lib/squid3' '--srcdir=.' '--disable-maintainer-mode' '--disable-dependency-tracking' '--disable-silent-rules' 'BUILDCXXFLAGS=-g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security -Wl,-Bsymbolic-functions -fPIE -pie -Wl,-z,relro -Wl,-z,now' '--datadir=/usr/share/squid' '--sysconfdir=/etc/squid' '--libexecdir=/usr/lib/squid' '--mandir=/usr/share/man' '--enable-inline' '--disable-arch-native' '--enable-async-io=8' '--enable-storeio=ufs,aufs,diskd,rock' '--enable-removal-policies=lru,heap' '--enable-delay-pools' '--enable-cache-digests' '--enable-icap-client' '--enable-follow-x-forwarded-for' '--enable-auth-basic=DB,fake,getpwnam,LDAP,NCSA,NIS,PAM,POP3,RADIUS,SASL,SMB' '--enable-auth-digest=file,LDAP' '--enable-auth-negotiate=kerberos,wrapper' '--enable-auth-ntlm=fake,smb_lm' '--enable-external-acl-helpers=file_userip,kerberos_ldap_group,LDAP_group,session,SQL_session,unix_group,wbinfo_group' '--enable-url-rewrite-helpers=fake' '--enable-eui' '--enable-esi' '--enable-icmp' '--enable-zph-qos' '--enable-ecap' '--disable-translation' '--with-swapdir=/var/spool/squid' '--with-logdir=/var/log/squid' '--with-pidfile=/var/run/squid.pid' '--with-filedescriptors=65536' '--with-large-files' '--with-default-user=proxy' '--enable-build-info=Ubuntu linux' '--enable-linux-netfilter' 'build_alias=x86_64-linux-gnu' 'CFLAGS=-g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security -Wall' 'LDFLAGS=-Wl,-Bsymbolic-functions -fPIE -pie -Wl,-z,relro -Wl,-z,now' 'CPPFLAGS=-Wdate-time -D_FORTIFY_SOURCE=2' 'CXXFLAGS=-g -O2 -fPIE -fstack-protector-strong -Wformat -Werror=format-security' '--with-openssl' '--enable-ssl' '--enable-ssl-crtd' '--enable-ltdl-convenience'
```

5. 인증서관련 작업
   - 인증서가 저장될 데이터베이스 생성하기

```
root@ubuntu:/opt/squid_certs# /usr/lib/squid/ssl_crtd -c -s /opt/squid_ssldb/ssl_db -M
40MB
Initialization SSL db...
Done
root@ubuntu:/opt/squid_certs# chown -R proxy.proxy /opt/squid_ssldb
```

   - Self Signed인증서 생성하기

: https가 redirect되어서 https로 연결될 때 이 인증서를 사용하기 때문에 IE에서 경고페이지가 나타남. 실제 구성하는 서버는 공인받은 인증서 등록이 필요할것으로 보임.

```
# openssl req -new -newkey rsa:2048 -days 36500 -nodes -x509 -keyout proxyCA.pem -out
proxyCA.pem
```

6. SQUID config파일 작성하기
   /etc/squid/squid.conf의 내용중에 설정된 값만 간추린 내용

```
acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

acl all src all
http_access allow all
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
http_access allow localhost
http_access deny all

http_port 3128
http_port 3127 intercept ← 3127/TCP은 http트래픽을 받을 포트
https_port       3129       intercept       ssl-bump       generate-host-certificates=on
dynamic_cert_mem_cache_size=4MB    cert=/opt/squid_certs/proxyCA.pem    ←    3129/TCP포트는
https트래픽을 받을 포트

ssl_bump stare all
sslcrtd_program  /usr/lib/squid/ssl_crtd -s /opt/squid_ssldb/ssl_db -M 40MB

cache_dir ufs /var/spool/squid 100 16 256
cache_store_log daemon:/var/log/squid/store.log
```

```
buffered_logs on
coredump_dir /var/spool/squid
pinger_enable off

wccp2_router 10.100.1.1 ← wccp가 설정된 라우터를 지정. SQUID서버와 연결된 인터페이스로 지정
wccp2_forwarding_method gre
wccp2_service standard 0
wccp2_service dynamic 70
wccp2_service_info 70 protocol=tcp flags=src_ip_hash,src_port_alt_hash priority=240 ports=443
← 70 인덱스번호는 라우터에서 wccp dynamic으로 정의한 번호와 매핑되어야 함.
```

7. 우분투서버에서 트래픽 Redirect시키기

iptables명령으로 http, https트래픽을 squid의 3127/TCP, 3129/TCP포트로 rediret되도록 아래와 같이 설정.

```
# iptables -t nat -A PREROUTING -i wccp0 -p tcp -m tcp --dport 80 -j DNAT --to-destination
10.100.1.100:3127
# iptables -t nat -A PREROUTING -i wccp0 -p tcp -m tcp --dport 443 -j DNAT --to-destination
10.100.1.100:3129
```

설정값 확인할때에는 iptables -t nat -L -n - v

8. SQUID데몬 실행하기

- squid데몬실행하기

  # /usr/sbin/squid

- 데몬 정상구동되었는지 확인

```
root@ubuntu:/home/sghan# ps -efw|grep squid
root      2468     1  0 15:56 ?        00:00:00 /usr/sbin/squid
proxy     2470  2468  0 15:56 ?        00:00:01 (squid-1)
proxy     2471  2470  0 15:56 ?        00:00:00 (ssl_crtd) -s /opt/squid_ssldb/ssl_db -M 40MB
proxy     2472  2470  0 15:56 ?        00:00:00 (ssl_crtd) -s /opt/squid_ssldb/ssl_db -M 40MB
proxy     2473  2470  0 15:56 ?        00:00:00 (ssl_crtd) -s /opt/squid_ssldb/ssl_db -M 40MB
proxy     2474  2470  0 15:56 ?        00:00:00 (ssl_crtd) -s /opt/squid_ssldb/ssl_db -M 40MB
proxy     2475  2470  0 15:56 ?        00:00:00 (ssl_crtd) -s /opt/squid_ssldb/ssl_db -M 40MB
proxy     2476  2470  0 15:56 ?        00:00:00 (logfile-daemon) /var/log/squid/access.log
proxy     2478  2470  0 15:56 ?        00:00:00 (logfile-daemon) /var/log/squid/store.log
root      3174  3161  0 16:10 pts/2    00:00:00 grep --color=auto squid
```

- Listenning포트 확인

```
root@ubuntu:/home/sghan# lsof -i -n
COMMAND  PID  USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
sshd    1039  root    3u  IPv4  15204      0t0  TCP *:ssh (LISTEN)
sshd    1039  root    4u  IPv6  15212      0t0  TCP *:ssh (LISTEN)
squid   2470 proxy    6u  IPv6  35179      0t0  UDP *:37248
squid   2470 proxy    7u  IPv4  35180      0t0  UDP *:55364
squid   2470 proxy   30u  IPv4  35197      0t0  UDP 10.100.1.100:2048->10.100.1.1:2048
squid   2470 proxy   31u  IPv6  35198      0t0  TCP *:3128 (LISTEN)
squid   2470 proxy   32u  IPv6  35199      0t0  TCP *:3127 (LISTEN)
squid   2470 proxy   33u  IPv6  35200      0t0  TCP *:3129 (LISTEN)
```

9. 라우터 wccp확인하기

우분투시스템이 squid와 wccp통신이 이루어지면 라우터에 Tunnel인터페이스가 생성된다는 로그메시지가 나타남. wccp의 상태와 터널 생성인터페이스를 확인함.

```
R1#show ip wccp
Global WCCP information:
    Router information:
        Router Identifier:                  192.168.10.151
        Protocol Version:                   2.0

    Service Identifier: web-cache
        Number of Service Group Clients:    1
        Number of Service Group Routers:    1
        Total Packets s/w Redirected:       4697
          Process:                          0
          CEF:                              4697
        Service mode:                       Open
        Service Access-list:                -none-
        Total Packets Dropped Closed:       0
        Redirect Access-list:               100
        Total Packets Denied Redirect:      0
        Total Packets Unassigned:           85
        Group Access-list:                  -none-
        Total Messages Denied to Group:     0
        Total Authentication failures:      0
        Total GRE Bypassed Packets Received: 0

    Service Identifier: 70
        Number of Service Group Clients:    1
        Number of Service Group Routers:    1
        Total Packets s/w Redirected:       18765
          Process:                          0
          CEF:                              18765
        Service mode:                       Open
        Service Access-list:                -none-
        Total Packets Dropped Closed:       0
        Redirect Access-list:               150
        Total Packets Denied Redirect:      0
        Total Packets Unassigned:           1013
        Group Access-list:                  -none-
        Total Messages Denied to Group:     0
        Total Authentication failures:      0
        Total GRE Bypassed Packets Received: 0

R1#show ip int brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                192.168.10.151  YES DHCP   up                    up
Ethernet0/1                10.100.1.1      YES NVRAM  up                    up
Ethernet0/2                10.200.1.1      YES NVRAM  up                    up
Ethernet0/3                unassigned      YES NVRAM  administratively down down
NVI0                       unassigned      YES unset  administratively down down
Tunnel0                    172.16.0.1      YES unset  up                    up
Tunnel1                    172.16.0.1      YES unset  up                    up
Tunnel2                    172.16.0.1      YES unset  up                    up
```