TECHNICOLOR CPE FIREWALL GUIDE

DATE: January 2011

VERSION: v1.0

ABSTRACT: This application note provides technical Firewall information and how this relates to the various Technicolor gateway products. In the definitions section a brief background on firewall concepts in general and the Technicolor CPE firewall in particular is presented. The subsequent section explains how to use the Technicolor CPE firewall.

APPLICABILITY: This application note applies to all Technicolor gateway products capable of using the Technicolor Stateful Firewall.

UPDATES Technicolor continuously develops new solutions, but is also committed to improve its existing products.

For more information on Technicolor's latest technological innovations, documents and software releases, visit us at www.technicolor.com

Table of Contents

1 Definitions

1.1 Firewall Concepts

Stateless Packet Filtering

Traffic filtering decisions are made based on a set of firewall rules. A firewall rule is a combination of traffic filters and an action. Each packet is checked against a set of firewall rules. When a firewall rule matches the packet's traffic parameters, the rule's action is executed. The rule's action can be to accept, drop, deny or log the packet.

Stateful Packet Filtering

How does a stateless packet filter become a stateful packet filter? When connections are tracked, the firewall can make stateful decisions and dynamically create firewall pinholes. Consequence of using a stateful packet filter is that the number of firewall rules to configure a certain firewall policy becomes smaller because connection tracking will relate packets belonging to each other (e.g. responses to requests).

Default Policy

When defining a security policy, one always starts from a well-defined default behaviour. This default behaviour can be expressed in two opposite ways: whitelisting and blacklisting.

Whitelisting

- Without explicit rules, the firewall blocks ALL traffic. Implementing a policy is done by adding firewall rules which accept wanted traffic.

Blacklisting

- Without explicit rules, the firewall accepts ALL traffic. Implementing a policy is done by adding firewall rules which block unwanted traffic.

From a security point-of-view the white listing default behaviour is highly preferred as all traffic is denied until explicitly allowed by adding firewall rules.

1.2 Technicolor CPE Firewall

The Technicolor CPE Firewall is a stateful inspection firewall, meaning that it uses connection tracking and packet inspection at application layer to take stateful decisions. The Technicolor CPE firewall filters IP traffic. Both IPv4 traffic filtering and IPv6 traffic filtering (for those products that support IPv6) are supported.

1.2.1 Hooks, chains and rules

Conceptually, the Technicolor CPE Firewall can be seen as a box filtering packet flows. Packet flows are classified according to the direction the CPE forwards packets. The flows identified by the firewall are:

- forward: traffic forwarded from an external or virtual interface to another external or virtual interface
- source: traffic originated by the CPE and forwarded to another interface
- sink: traffic destined to the CPE

In firewall context the policy for each flow type is managed by a set of firewall rules associated with a firewall hook. Such hooks are named after the flow type, i.e. forward, source and sink:

Firewall rules are contained in chains. A rule contains filter criteria based on protocol parameters (e.g. IP protocol) and meta-data (e.g. source interface), and an action (e.g. accept, drop). A firewall rule can also link to a chain with a different set of rules. This way, chains can be linked together to form a hierarchy of chains containing firewall rules.

An example of such a hierarchy of linked chains shown per firewall hook:

- sink
  - sink_fire
  - sink_system_service
- forward
  - forward_multicast
  - forward_fire
  - forward_timeofday
  - forward_host_service
  - forward_custom
  - forward_level
  - forward_portmapping
- source
  - source_fire
  - source_system_service

1.2.2 Default Firewall Policy

When no firewall rules are configured, a default firewall policy applies per firewall hook:

hook	default policy
forward	drop all traffic
sink	drop all traffic
source	accept all traffic

For all traffic flows except originated by the CPE, a whitelisting default policy behaviour is implemented which is the best practice with respect to security.

For all traffic originated by the CPE, a blacklisting default policy is chosen which means services on the CPE generating traffic are implicitly trusted.

1.2.3 Firewall Modules

Applications exist on the CPE which need to manage firewall rules. A Good example is UPnP which opens pinholes to allow traffic from the Internet to applications running on LAN devices. Applications needing to manage firewall rules allocate a module in the firewall. A dedicated chain is given to that application to manage its firewall policy.

1.2.4 Firewall Levels

Firewall Levels is a concept which can be compared with a global security switch with a predefined number of security levels ranging from a very strict security policy to no security at all.

Each firewall level has an associated set of firewall rules expressing the level security policy. By activating a specific firewall level, the firewall is reconfigured with the firewall rules belonging to the configured firewall level. The firewall level concept in the Technicolor CPE is fully customizable via CLI.

Firewall levels only define a security policy for forwarded traffic; traffic to the CPE is managed via system services. See the "Technicolor CPE Firewall Management" section for a detailed explanation.

A typical example of firewall levels defined for CPE products:

Level	Description
High	Use this Security Level to block all outgoing connections except well known applications (DNS, HTTP, HTTPS, FTP, TELNET, IMAP, and POP) and block all incoming connections. Game and Application sharing is not allowed by the firewall.
Medium	Use this Security Level to allow all outgoing connections except Windows protocols (NetBIOS, RPC, SMB) and block all incoming connections. Game and Application sharing is allowed by the firewall.
Standard	Use this Security Level to allow all outgoing connections and block all incoming traffic. Game and Application sharing is allowed by the firewall.
Low	Use this Security Level to allow all outgoing connections and block all incoming traffic except Internet Control Message Protocol (ICMP). Game and Application sharing is allowed by the firewall.
Disabled	Disable the firewall. All traffic is allowed to pass through your gateway. Game and Application sharing is allowed by the firewall.
BlockAll	Use this Security Level to block all traffic from and to the Internet. Game and Application sharing is not allowed by the firewall.

Typically, the CPE is deployed with NAT enabled for IPv4. As NAT by default blocks unsolicited inbound traffic coming from the Internet, NAT is often used to perform the firewall function and the firewall level in such situation is often set to Disabled. This means that the firewall actually allows all traffic and NAT is counted on to implement a security policy.

As IPv6 is deployed without NAT support, the firewall becomes the single entity enforcing a security policy. By default the Technicolor CPE products supporting IPv6 will be deployed with firewall level set to 'Standard'. This means that traffic to the Internet will be allowed, but unsolicited inbound traffic from the Internet will be blocked.

2 Technicolor CPE Firewall Management

2.1 Global Firewall Settings

Global firewall settings can be configured with the :firewall config command.

Firewall parameters:

state	Disable/Enable the firewall
keep	Disable/Enable keeping existing connections when firewall policy changes
tcpchecks	Disable/Enable TCP protocol checks and define sequence number tracking algorithm
udpchecks	Disable/Enable UDP protocol checks
icmpchecks	Disable/Enable ICMP protocol checks
logdefault	Disable/Enable logging when default firewall policy is used
logthreshold	Disable/Enable rate limiting of logging
tcpwindow	Define TCP window for sequence number tracking (when tcpchecks=fast)

Enable the firewall:

```
:firewall config state=enabled
```

When firewall state is disabled, no filtering is done and all traffic is allowed!

2.2 Firewall Chains

To list all firewall chains:

```
:firewall chain list
```

To add a firewall chain:

```
:firewall chain add chain=<name of the chain>
```

2.3 Firewall Rules

To list firewall rules:

```
:firewall rule list
```

To add a firewall rule:

```
:firewall rule add   chain = <chain name>
     The name of the chain which contains the rule.
   [index = <number>]
     The index of the rule in the chain.
   [name = <string>]
     The name of the new rule.
   [clink = <chain name>]
     The name of the chain to be parsed when this rule applies.
   [srcintf [!]= <{wan|local|lan|tunnel|dmz|guest}>]
     The name of the source interface expression.
   [srcip [!]= <{private|ssdp_ip|mdap_ip}>]
     The name of the source ip expression.
   [dstintf [!]= <{wan|local|lan|tunnel|dmz|guest}>]
     The name of the destination interface expression.
   [dstip [!]= <{private|ssdp_ip|mdap_ip}>]
     The name of the destination ip expression.
   [serv [!]= <{icmp|igmp|ftp|telnet|http|httpproxy|https|RPC|NBT|SMB|imap|
              imap3|imap4-ssl|imaps|pop2|pop3|pop3s|smtp|ssh|dns|nntp|ipsec|
              esp|ah|ike|sip|h323|dhcp|rtsp|ssdp_serv|mdap_serv|syslog|VoIP-
              Inc-SIP-UDP|VoIP-Inc-SIP-TCP|VoIP-Inc-RTP|icmpv6}>]
     The name of the service expression.
   [length [!]= <{}>]
     The name of the length expression.
   [log = <{disabled|enabled}>]
     Disable/Enable logging when this rule applies.
   [state = <{disabled|enabled}>]
     Disable/Enable this rule.
   action = <{accept|deny|drop|reset|count|link}>
     The action to be taken when this rule applies ('link' when clink is used).
```

Example: add a rule allowing all forwarded traffic:

```
:firewall rule add chain=forward index=1 action=accept
```

Some firewall rule parameters refer to expressions. Expressions are filter objects which are defined within the **`:expr`** CLI topic.

- srcintf and dstintf refer to interface expressions
- srcip and dstip refer to IPv4/IPv6 address expressions
- serv refers to service expressions
- length refers to length expressions

2.4 Expressions

To list expressions:

```
:expr list
```

To add an expression:

```
:expr add  name = <{wan|local|lan|tunnel|dmz|guest|private|ssdp_ip|mdap_ip|icmp|igmp|
          ftp|telnet|http|httpproxy|https|RPC|NBT|SMB|imap|imap3|imap4-ssl|
          imaps|pop2|pop3|pop3s|smtp|ssh|dns|nntp|ipsec|esp|ah|ike|sip|h323|
```

```
        dhcp|rtsp|ssdp_serv|mdap_serv|syslog|VoIP-Inc-SIP-UDP|VoIP-Inc-SIP-
        TCP|VoIP-Inc-RTP|icmpv6}>
  The name of an expression to add.
[type = <{intf|ip|serv|mac|length}>]
  The type of an expression.
mac [!]= <hardware-address>
  The MAC address.
addr [!]= <ip-range>
  The IP address or range.
[mask [ <ip-mask(dotted or cidr)>]
  The IP mask (ignored if an IP range is provided).
[intf [!]= <{loop|Internet|lan1|wan1|dmz1|guest1|loop|Internet|lan1|wan1|
          dmz1|guest1}>]
  The IP interface name.
[intfgroup [!]= <{wan|local|lan|tunnel|dmz|guest}>]
  The IP interface group.
[tos [!]= <number{0-255}>]
  The Type Of Service specification in the IP packet.
[precedence [!]= <{routine|priority|immediate|flash|flash-override|CRITIC-
                ECP|internetwork-control|network-control} or number>]
  The precedence in the IP packet (part of tos).
[dscp [!]= <{ef|af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43|
          cs0|cs1|cs2|cs3|cs4|cs5|cs6|cs7} or number>]
  The diffserv code point in the IP packet (part of tos).
[proto [!]= <{icmp|icmpv6|igmp|ipinip|tcp|udp|ah|esp|ipcomp} or number>]
  The IP protocol (name or number) in the IP packet.
[srcport [!]= <{undefined|at-echo|at-nbp|at-rtmp|at-zis|auth|bgp|biff|
              bootpc|bootps|chargen|clearcase|daytime|discard|dns|domain|
              doom|echo|exec|finger|ftp|ftp-data|gopher|h323|httpproxy|ike|
              ils|imap2|imap3|ingres-net|ipcserver|ipx|irc-o|irc-u|kerberos|
              ldap|login|netbios-dgm|netbios-ns|netbios-ssn|netwall|netware-
              ip|new-rwho|nfds|nicname|nntp|ntalk|ntp|pcmail-srv|pop2|pop3|
              printer|qotd|realaudio|rip|rtelnet|rtsp|sip|smtp|snmp|
              snmptrap|snpp|sntp|sql*net|sql-net|sqlserv|sunrpc|syslog|
              systat|talk|telnet|time|timed|tftp|ulistserv|utime|uucp|uucp-
              rlogin|who|www-http|whoami|xwindows} or number>]
  The TCP/UDP source port number or range begin.
[srcportend = <{undefined|at-echo|at-nbp|at-rtmp|at-zis|auth|bgp|biff|
              bootpc|bootps|chargen|clearcase|daytime|discard|dns|domain|
              doom|echo|exec|finger|ftp|ftp-data|gopher|h323|httpproxy|ike|
              ils|imap2|imap3|ingres-net|ipcserver|ipx|irc-o|irc-u|kerberos|
              ldap|login|netbios-dgm|netbios-ns|netbios-ssn|netwall|netware-
              ip|new-rwho|nfds|nicname|nntp|ntalk|ntp|pcmail-srv|pop2|pop3|
              printer|qotd|realaudio|rip|rtelnet|rtsp|sip|smtp|snmp|
              snmptrap|snpp|sntp|sql*net|sql-net|sqlserv|sunrpc|syslog|
              systat|talk|telnet|time|timed|tftp|ulistserv|utime|uucp|uucp-
              rlogin|who|www-http|whoami|xwindows} or number>]
  The TCP/UDP source port range end. (inclusive)
[dstport [!]= <{undefined|at-echo|at-nbp|at-rtmp|at-zis|auth|bgp|biff|
              bootpc|bootps|chargen|clearcase|daytime|discard|dns|domain|
              doom|echo|exec|finger|ftp|ftp-data|gopher|h323|httpproxy|ike|
              ils|imap2|imap3|ingres-net|ipcserver|ipx|irc-o|irc-u|kerberos|
              ldap|login|netbios-dgm|netbios-ns|netbios-ssn|netwall|netware-
              ip|new-rwho|nfds|nicname|nntp|ntalk|ntp|pcmail-srv|pop2|pop3|
              printer|qotd|realaudio|rip|rtelnet|rtsp|sip|smtp|snmp|
              snmptrap|snpp|sntp|sql*net|sql-net|sqlserv|sunrpc|syslog|
              systat|talk|telnet|time|timed|tftp|ulistserv|utime|uucp|uucp-
              rlogin|who|www-http|whoami|xwindows} or number>]
  The TCP/UDP destination port number or range begin.
[dstportend = <{undefined|at-echo|at-nbp|at-rtmp|at-zis|auth|bgp|biff|
              bootpc|bootps|chargen|clearcase|daytime|discard|dns|domain|
              doom|echo|exec|finger|ftp|ftp-data|gopher|h323|httpproxy|ike|
              ils|imap2|imap3|ingres-net|ipcserver|ipx|irc-o|irc-u|kerberos|
              ldap|login|netbios-dgm|netbios-ns|netbios-ssn|netwall|netware-
              ip|new-rwho|nfds|nicname|nntp|ntalk|ntp|pcmail-srv|pop2|pop3|
              printer|qotd|realaudio|rip|rtelnet|rtsp|sip|smtp|snmp|
              snmptrap|snpp|sntp|sql*net|sql-net|sqlserv|sunrpc|syslog|
              systat|talk|telnet|time|timed|tftp|ulistserv|utime|uucp|uucp-
              rlogin|who|www-http|whoami|xwindows} or number>]
  The TCP/UDP destination port range end.
[icmptype [!]= <{destination-unreachable|time-exceeded|parameter-problems|
               source-quench|redirect|packet-too-big|router-renumbering|
               echo-request|echo-reply|router-advertisement|router-
               solicitation|timestamp-request|timestamp-reply|information-
               request|information-reply|address-mask-request|address-mask-
               reply|multicast-listener-query|multicast-listener-report|
               multicast-listener-done|neighbor-advertisement|neighbor-
               solicitation|node-information-query|node-information-
               response|inverse-neighbor-solicitation|inverse-neighbor-
               advertisement|v2-multicast-listener-report|home-agent-
               address-request|home-agent-addres-reply|mobile-prefix-
               solicitation|mobile-prefix-advertisement|certification-path-
               solicitation|certification-path-advertisement|...} or
               number>]
  The ICMP type (name or number) of the packet.
[icmpcode [!]= <number{0-15}>]
  The ICMP code or range begin.
[icmpcodeend = <number{0-15}>]
  The ICMP code range end. (inclusive)
iplengthmin [!]= <number>
  The minimum IP length in bytes (header inclusive).
[iplengthmax = <number>]
  The maximum IP length including header in bytes (header inclusive).
```

Example: add a rule allowing all traffic coming from the LAN to the CPE telnet service:

```
:expr add name=lan type=intf intfgroup=lan
:expr add name=telnet type=serv proto=tcp dstport=23
:firewall rule add chain=sink index=1 srcintf=lan serv=telnet action=accept
```

2.5 System Services

Services running on the CPE system require configuration of NAT portmaps and firewall rules to allow connectivity to and from those services. To avoid tedious NAT and firewall configuration per service, each service can be managed via the system service CLI and appropriate NAT and firewall configuration is automatically applied.

To list system services:

```
:service system list
```

To modify system service configuration:

```
:service system modify  name = <name of the service>
     The name of the service.
   [state = <{disabled|enabled}>]
     Disable/Enable this service.
   [port = <{undefined|at-echo|at-nbp|at-rtmp|at-zis|auth|bgp|biff|bootpc|
           bootps|chargen|clearcase|daytime|discard|dns|domain|doom|echo|exec|
           finger|ftp|ftp-data|gopher|h323|httpproxy|ike|ils|imap2|imap3|
           ingres-net|ipcserver|ipx|irc-o|irc-u|kerberos|ldap|login|netbios-
           dgm|netbios-ns|netbios-ssn|netwall|netware-ip|new-rwho|nfds|nicname|
           nntp|ntalk|ntp|pcmail-srv|pop2|pop3|printer|qotd|realaudio|rip|
           rtelnet|rtsp|sip|smtp|snmp|snmptrap|snpp|sntp|sql*net|sql-net|
           sqlserv|sunrpc|syslog|systat|talk|telnet|time|timed|tftp|ulistserv|
           utime|uucp|uucp-rlogin|who|www-http|whoami|xwindows} or number>]
     The port of the service.
   [dynportrange = <port-range>]
     The dynamic port range for this service.
   [qoslabel = <{None|Interactive|Management|SIPS_RTP|SIPS_SIG|Video|VoIP-RTP|
              VoIP-Signal|default}>]
     QOS label for service data.
   [routelabel = <{None|Interactive|Management|SIPS_RTP|SIPS_SIG|Video|VoIP-
                RTP|VoIP-Signal|default}>]
     Route label for service data.
   [srcintf <{loop|Internet|lan1|wan1|dmz1|guest1}>]
     The primary IP interface for this service.
   [log = <{disabled|enabled}>]
     Disable/Enable service logging.
   [forward = <{disabled|enabled}>]
     Disable/Enable service forwarding.
   [natpmweight = <number{0-255}>]
     The nat portmap weight for this service.
```

To add an interface or interface group to the service access list:

```
:service system ifadd  name = <name of the service>
     The name of the service for this access list.
   [group = <{wan|local|lan|tunnel|dmz|guest} or number>]
     The interface group for this access list.
   [intf = <{loop|Internet|lan1|wan1|dmz1|guest1}>]
     The interface for this access list.
```

To add an IP address (IPv4 or IPv6) to the service access list:

```
:service system ipadd  name = <{name of the service>
     The name of the service for this access list.
   ip = <ip-range>
     The IP address (range) for this access list.
```

Example: add a rule allowing all traffic coming from the LAN to the CPE telnet service:

```
:service system ifadd name=TELNET group=lan
```

2.6 Host Services

Services running on the LAN devices require configuration of NAT portmaps and firewall rules to allow connectivity to and from those services. To avoid tedious NAT and firewall configuration per host service, each service can be managed via the host service CLI and appropriate NAT and firewall configuration is automatically applied.

To list host services:

```
:service host list
```

To add host service configuration:

```
:service host add  name = <quoted string>
     The name of the service.
   [mode = <{server|client|custom}>]
     server, client or custom service ?
   [category = <>]
     The category to which the service belongs.
```

To assign a service to a host:

```
:service host assign  name = name of the service>
     The name of the service.
   [host = <ip-address>]
     The IP address of the host.
   [log = <{disabled|enabled}>]
     Enable/disable logging.
```

Example: assign an FTP service to device with IP address 192.168.1.5 on a LAN device:

```
add name="FTP Server"
assign name="FTP Server" host=192.168.1.5
```

2.7 Firewall Levels

Firewall Levels implement a fully customizable security slider with well-defined security levels.

To list firewall levels:

```
:firewall level list
```

To add a firewall level:

```
:firewall level add     name = <string>
     The name of the security level to add.
   [index = <number>]
     The index of the security level.
   [readonly = <{disabled|enabled}>]
     Select whether the security level is readonly in GUI
   [udptrackmode = <{strict|loose}>]
     Select UDP connection tracking mode.
   [service = <{disabled|enabled}>]
     Enable/Disable host service definitions for this security level.
   [proxy = <{disabled|enabled}>]
     Enable/Disable proxy system services for this security level.
   [text = <quoted string>]
     The description of this security level.
   [policy = <{default|drop|accept}>]
     Select default policy of this security level.
```

Example: add a firewall level.

```
:firewall level add name=Management text="Use this security level to only allow Management traffic" policy=default
```

Adding a firewall level will result in a firewall chain called "forward_level_Management" where the related firewall rules can be defined:

```
:expr add name=telnet type=serv proto=tcp dstport=23
:firewall rule add chain=forward_level_Management index=1 serv=telnet action=accept
```

To active a specific firewall level:

```
:firewall level set  [name = <security level nam>]
     The name of the security level to set active.
```

Example: set Management level as active level

```
:firewall level set name=Management
```

END OF DOCUMENT