WAN Optimization Configuration
(FortiOS 5.0 and 5.2)

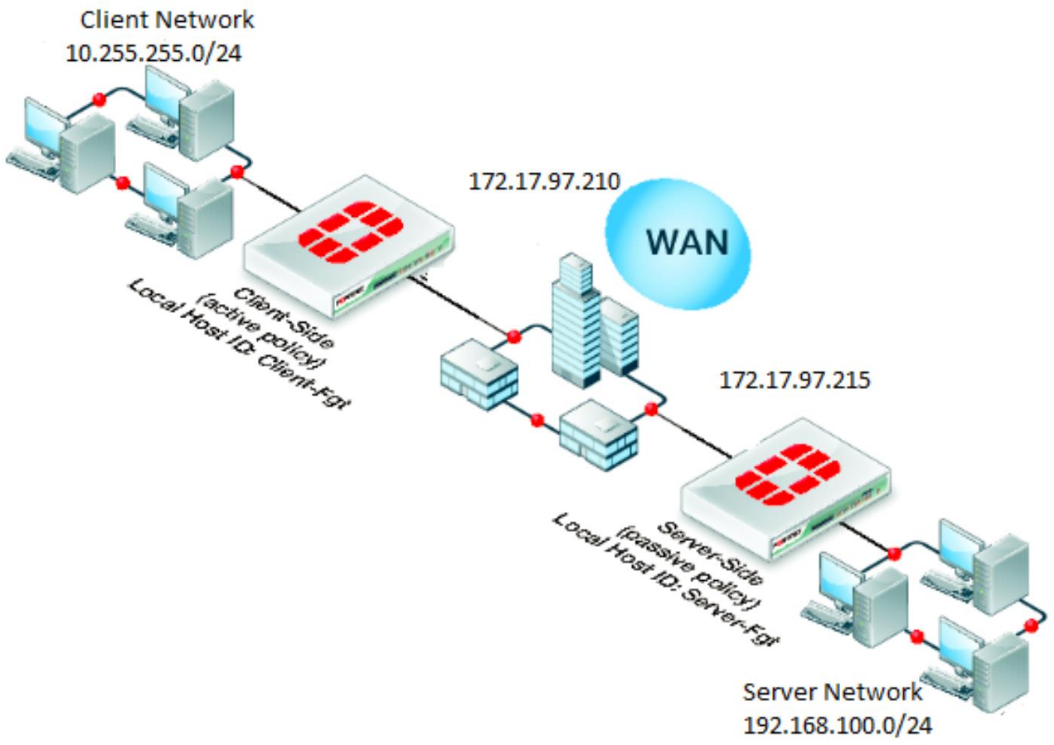
Client/Server Architecture:

Traffic across a WAN typically consists of clients on a client network communicating across a WAN with a remote server network. These communication sessions can be open text over the WAN or they can be encrypted by SSL VPN or IPsec VPN

Client/Server architecture Topology

This example configuration includes an Active-Passive WAN optimization with secure tunneling over IPSec VPN. The IPSec tunnel has already been configured and is functional. WAN optimization is added afterward.

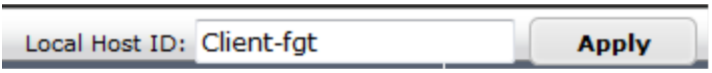
The Client-side FortiGate is 200D and Server-side FortiGate is 240D



Configuration steps:

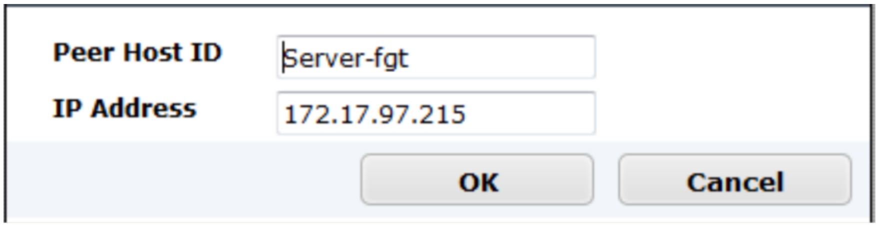
1) Configure the client-side FortiGate unit:

- ❖ Go to WAN Opt. & Cache > WAN Opt. Peers > Peers
  - ➢ Enter a Local Host ID for the client-side FortiGate unit as Client-fgt
    - :



Local Host ID: Client-fgt

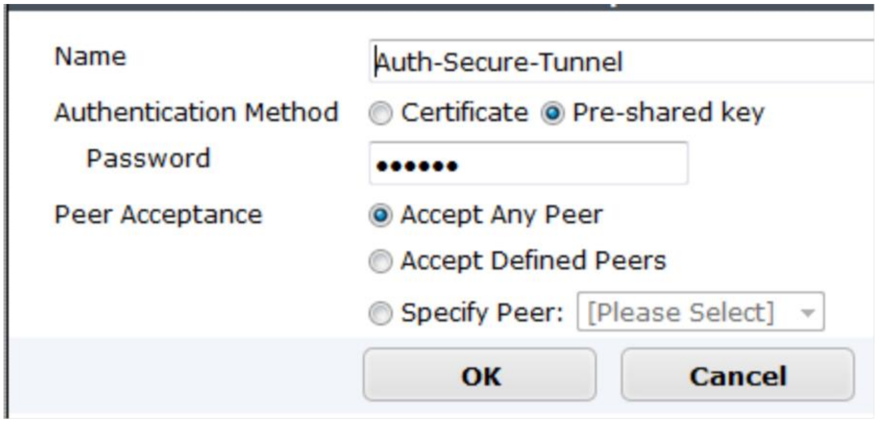
  - ➢ Select Create New and add a Peer Host ID and the IP Address for the server-side FortiGate



Peer Host ID: Server-fgt

IP Address: 172.17.97.215

- ❖ Go to WAN Opt & Cache > WAN Opt. Peers > Authentication Groups
  - ➢ Select Create New to add the authentication group to be used for secure tunneling



Name: Auth-Secure-Tunnel

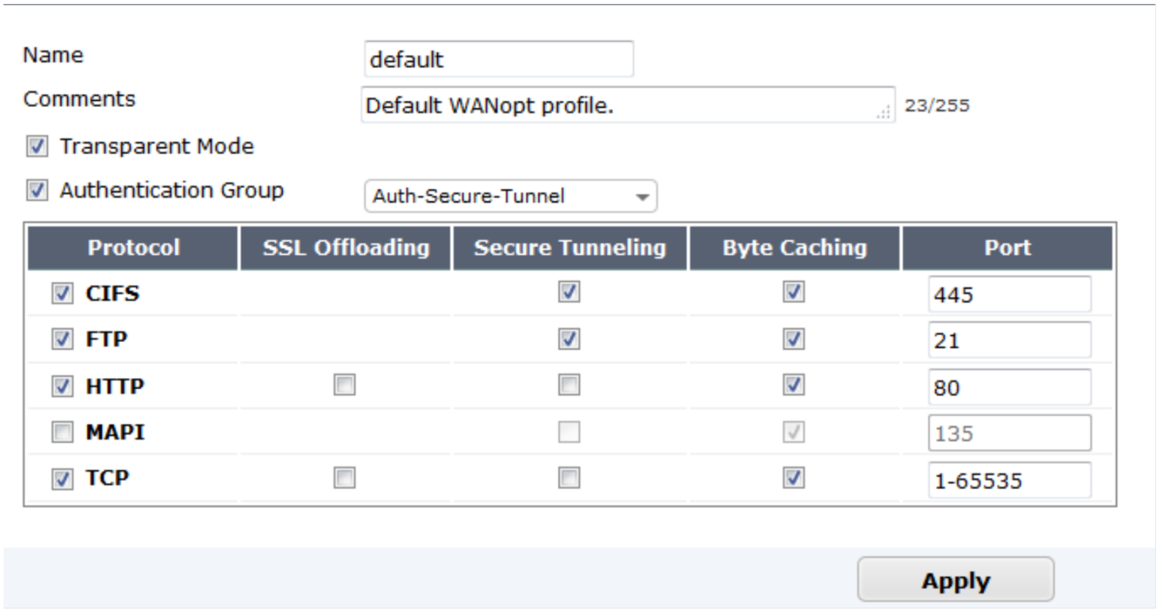
Authentication Method: ○ Certificate ● Pre-shared key

Password: ••••••

Peer Acceptance: ● Accept Any Peer ○ Accept Defined Peers ○ Specify Peer: [Please Select]

- ❖ Go to WAN Opt. & Cache > WAN Opt. Profiles > Profiles
  - ➢ Select Create New to add a WAN Optimization profile that enables secure tunneling and includes the authentication group
  - ➢ Select any protocol for optimization

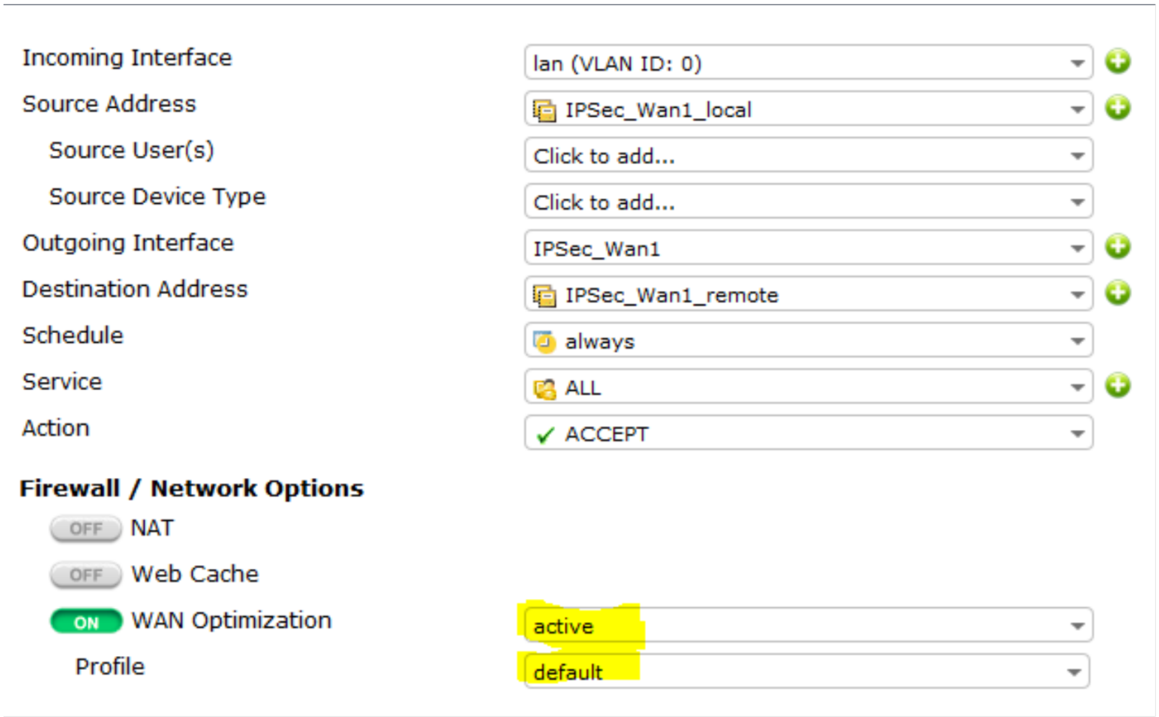
- ➢ Select Transparent mode -- this will source your traffic as Client address
- ➢ Select Authentication group name



Name	default
Comments	Default WANopt profile. 23/255
☑ Transparent Mode	
☑ Authentication Group	Auth-Secure-Tunnel

Protocol	SSL Offloading	Secure Tunneling	Byte Caching	Port
☑ CIFS		☑	☑	445
☑ FTP		☑	☑	21
☑ HTTP	□	□	☑	80
□ MAPI		□	☑	135
☑ TCP	□	□	☑	1-65535

- ❖ Go to Policy & Objects > Objects > Addresses
  - ➢ Select "Create New" to add a Firewall address for the client and server respectively.
- ❖ Go to Policy & Objects > Policy > IPv4
  - ➢ Select "Create New" to add an active WAN optimization security policy



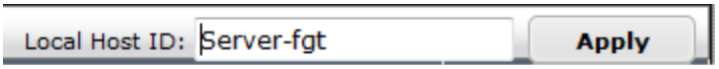
Incoming Interface	lan (VLAN ID: 0)
Source Address	IPSec_Wan1_local
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	IPSec_Wan1
Destination Address	IPSec_Wan1_remote
Schedule	always
Service	ALL
Action	✓ ACCEPT

Firewall / Network Options

OFF NAT	
OFF Web Cache	
ON WAN Optimization	active
Profile	default

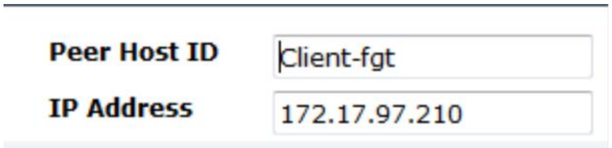
This policy is from Internal interface to IPSec tunnel interface with WAN optimization enabled with active state and required authentication profile which in this case is default.

2) Configure Server-side FortiGate unit:

- Go to WAN Opt. & Cache > WAN Opt. Peers > Peers
  - Enter a Local Host ID for the server-side FortiGate unit
    - 

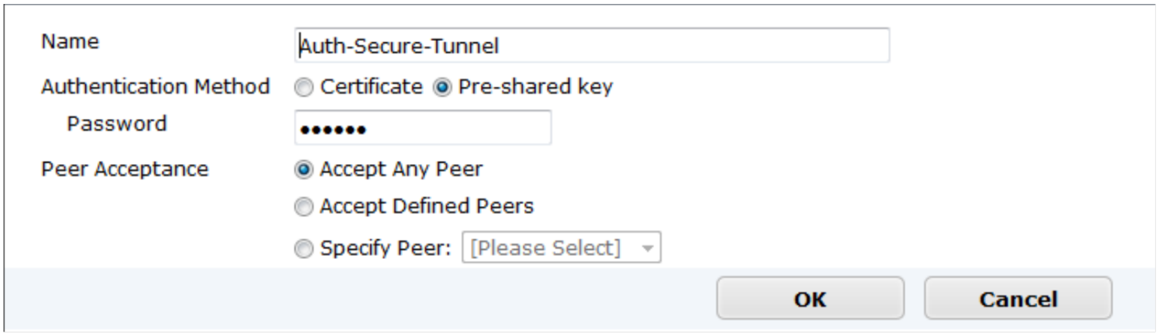
      Local Host ID: Server-fgt

  - Select Create New and add a Peer Host ID and the IP Address for the client-sideFortiGate:



Peer Host ID	Client-fgt
IP Address	172.17.97.210

- Go to Wan Opt. & Cache > WAN Opt. Peers > Authentication Groups
  - Select Create new and add an authentication group to be used for secure tunneling:



Name: Auth-Secure-Tunnel

Authentication Method: ○ Certificate ● Pre-shared key

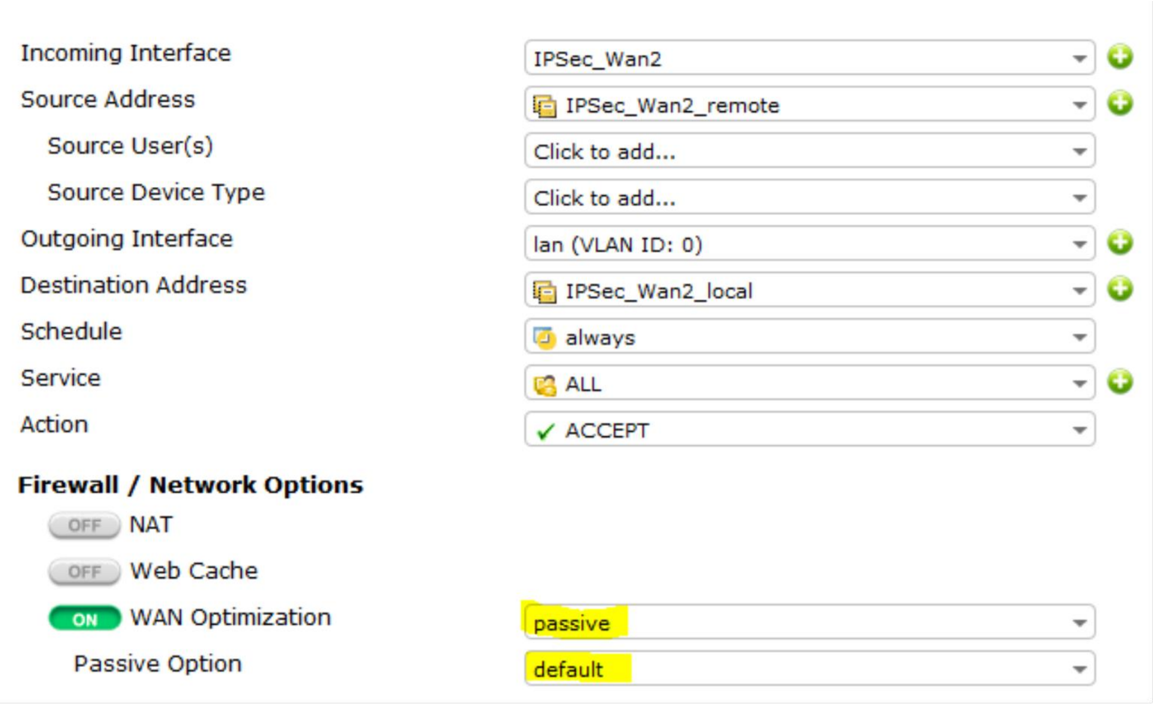
Password: ••••••

Peer Acceptance: ● Accept Any Peer

○ Accept Defined Peers

○ Specify Peer: [Please Select]

- Go to Policy & Objects > Objects > Addresses
    - Select "Create New" to add a Firewall address for the client and server respectively.
- Create a passive WAN optimization policy that applies application control



Incoming Interface	IPSec_Wan2
Source Address	IPSec_Wan2_remote
Source User(s)	Click to add...
Source Device Type	Click to add...
Outgoing Interface	lan (VLAN ID: 0)
Destination Address	IPSec_Wan2_local
Schedule	always
Service	ALL
Action	✓ ACCEPT

Firewall / Network Options

OFF NAT

OFF Web Cache

ON WAN Optimization: passive

Passive Option: default

This policy is from IPSec interface to the Internal interface of the server-side FortiGate with WAN optimization enabled with passive state.

- From the CLI enter the following command to add a WAN optimization tunnel explicit proxy policy.

```
configure firewall explicit-proxy-policy

        edit 1

                set proxy wanopt
                set dstintf port1
                set srcaddr all
```

```
            set dstaddr all
            set action accept
            set schedule always
            set service ALL

    end
```

IMP------> Secure Tunneling:

In Active-Passive WAN optimization
Select “Enable Secure Tunnel” only in the active rule.

In Peer-to-Peer WAN optimization
Select “Enable Secure Tunnel” in the WAN optimization rule on both FortiGate units.

Troubleshooting WAN optimization

1) Browse from a PC on the client network browse to the IP address of a web server network http://192.168.100.111. You should be able to connect over the WAN optimization tunnel.

2) Check WAN Opt. & Cache > Monitor it will show the protocol that has been optimized and the reduction rate in WAN bandwidth usage.

If you cannot connect

- Try the following diagnose commands on FortiGate client or server
- Confirm the policy on client-side and server-side unit
- Check routing on the FortiGate units to make sure packets can be forwarded as required.
  e.g., You should be able to ping the internal network behind the client-side/server-side FortiGate.

Diagnostic Tools

A) CLI commands with sample output:

```
FG240D-Server # diagnose wad tunnel list

Tunnel: id=2245 type=auto
  vd=0 shared=no uses=1 state=2
  peer name=Client-fgt id=1776 ip=172.17.97.210
  SSL-secured-tunnel=no auth-grp=Auth-Secure-Tunnel
  bytes_in=0 bytes_out=0
Tunnels total=1 manual=0 auto=1
```

```
FG240D-Server # diagnose wad history list TCP 10

stats history vd=0 proto=tcp period=last 10min

         --- LAN ---                  --- WAN ---

   bytes_in      bytes_out      bytes_in      bytes_out

  ------------   -------------   ------------   -------------

     0             0             0             0
    2951          5965          8385          5787
    1924          3733          5173          3920
    6414         11902         16710          12390
…
```

```
FG240D-Server # diagnose wad stats

summary

 sessions total=1767 active=0 max=9

crypto

 software

  enc total 58 active 0 max 1
  dec total 62 active 0 max 1
…

 hardware

  enc total 1089 active 0 max 1
  dec total 1108 active 0 max 1
…

Tunnels
 http tunnel
  bytes_in=46757 bytes_out=55162

 ftp tunnel
```

```
    bytes_in=0 bytes_out=0

  cifs tunnel
    bytes_in=116511 bytes_out=112450

  mapi tunnel
    bytes_in=0 bytes_out=0

  tcp tunnel
    bytes_in=258547 bytes_out=187041

  maintenance
    bytes_in=305405 bytes_out=141900

http

  LAN:
    bytes_in=12662 bytes_out=178263

  WAN:
    bytes_in=46757 bytes_out=55162

ftp

  LAN:
    bytes_in=0 bytes_out=0

  WAN:
    bytes_in=0 bytes_out=0

cifs

  LAN:
    bytes_in=54055 bytes_out=60417

  WAN:
    bytes_in=116511 bytes_out=112450

mapi

  LAN:
    bytes_in=0 bytes_out=0

  WAN:
    bytes_in=0 bytes_out=0

tcp

  LAN:
    bytes_in=95389 bytes_out=182923

  WAN:
    bytes_in=258547 bytes_out=187041
```

```
FG240D-Server # diagnose wad session list

Session: svr-side auto-detected 10.255.255.100:52468->192.168.100.111:80
   id=407974 vd=0 fw-policy=4
   state=3 app=http sub_type=0 dd_mode=3 dd_method=3
   SSL disabled
   WAN-side: to-client

      Tunnel Port:
         state=2 session_id=2101540166 remote_sid=244981077
         tunnel id=2252 SSL-secured=no peer=Client-fgt auth-grp=Auth-Secure-Tu
nnel
         buf_blocked=0 buf_block_threshold=2097152
         bytes_unconfirm_rcv=0 bytes_unconfirm_snd=0

   LAN-side: to-server

      TCP Port:
         state=2 r_blocks=0 w_blocks=0 read_blocked=0
         bytes_in=0 bytes_out=0 shutdown=0x0

Sessions total=1
```

B) List of Relevant Diagnostics commands

diagnose wad tunnel list --> will show you the established tunnels

get test wad 11 -- > Use this command on the FortiGate client to see the details about WAN opt and statistics

diag wacs stats >>>> Displays web cache statistics

diag wacs recents >>>> Displays recent web cache database activity

get test wad cifs

get test wad 50 --> display Web Cache stats

get test wad 53 --> to display firewall policies

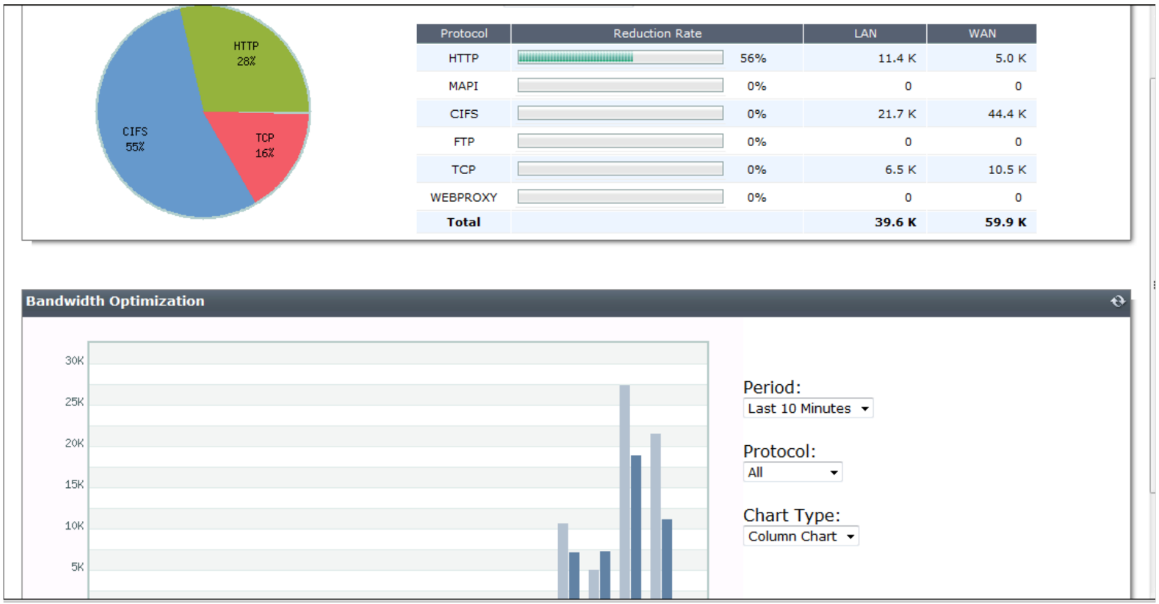
diagnose sys wccp list

diagnose debug application wad -1 -----> will show you the detailed information

diagnose sys session filter dport 7810

diagnose snipper packet any "port 7810" 4

C) WAN Monitor



Protocol	Reduction Rate	LAN	WAN
HTTP	56%	11.4 K	5.0 K
MAPI	0%	0	0
CIFS	0%	21.7 K	44.4 K
FTP	0%	0	0
TCP	0%	6.5 K	10.5 K
WEBPROXY	0%	0	0
Total		**39.6 K**	**59.9 K**

Period: Last 10 Minutes

Protocol: All

Chart Type: Column Chart

The reduction rate in traffic shaping ensures that WAN optimization for that particular protocol is optimized.