

Designing the Perfect Network Firewall & Understanding Network Routing

Adam Schechter
Precision Consulting



MACTECH



MACTECH



MACTECH

Configuring a Top Performing Network Firewall













- Top brands and models in use today
- Basic firewall
- Most common advanced settings
- Troubleshooting the stuff you got wrong





Apps

Config

-  **Virus Blocker** Install
-  **Virus Blocker Lite** Install
-  **Spyware Blocker** Install
-  **Spam Blocker** Install
-  **Phish Blocker** Install
-  **Bandwidth Control** Install
-  **Application Control** Install
-  **Application Control Lite** Install
-  **Ad Blocker** Install
-  **WAN Failover** Install
-  **WAN Balancer** Install
-  **IPsec VPN** Install

Default Rack

Tx: 67.02KB/s
Rxc: 297.14KB/s

493

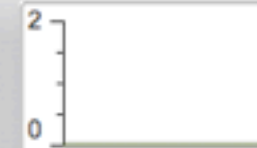
low

F: 2935.81 MB
U: 667.04 MB

Network Sessions CPU Load

Web Filter

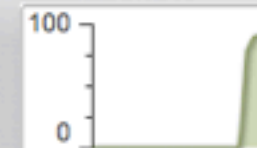
Settings Help



Pages scanned
Pages blocked
Pages passed
Passed by policy

Web Cache

Settings Help



Cache hits
Cache misses
User Bypass
System Bypass

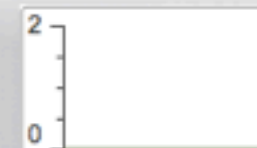
Firewall

Settings Help

Sessions passed
Sessions logged
Sessions blocked
Current Sessions

Intrusion Prevention

Settings Help



Sessions scanned
Sessions logged
Sessions blocked
Current Sessions

Services

Reports

Settings Help

Policy Manager

Settings Help

Directory Connector

Settings Help

Captive Portal

Settings Help

Sessions blocked
Clients authorized

OpenVPN

Settings Help

Sessions passed
Clients Connected

Attack Blocker

Sessions accepted
Sessions limited
Sessions dropped

Number of Processors / Type / Speed:
2, Intel(R) Pentium(R) CPU G640 @ 2.80GHz,
2793.699
Load average (1 min, 5 min, 15 min):
0.66, 0.2, 0.11
Tasks (Processes)
106
Uptime:
2 Hours, 50 Minutes

Some Top Brands

	Modular	License	VPN	DNS Handling	Support
Cisco	Yes	\$\$\$	Built in, Mac Client	DNS Reply Modification	Paid
Sonicwall	cli	\$\$\$	IPSecuritas		Paid
Netgear	no	\$	IPSecuritas	No	Free
Zyxel	cli	\$	IPSecuritas	Forward	Free
Kerio	partial	\$\$	Mac Client	Easy	Resellers: free
DD-WRT	cli	\$0	Built in	Easy	Forums
PFSense	Yes	\$0	Built in	Yes	Forums
Airport	No	1 time	Pass through	None	AppleCare

WAN Routing

- Static vs Dynamic Addressing
- Multiple IP Addresses
- Bonding IP addresses

Port Forwarding

- What is a port
- Forwarding ports into a given device
- NAT Rules direct traffic
- Firewall Rules allow/deny based on path

DNS Considerations

- Who's providing DNS
 - Server vs Hardware
- Loopback, local DNS,
 - Prevents the need for a full DNS

VPN Connectivity

- VPN clients - and not wanting to have to deal with them, was the impetus for my deep research into routers.
- Flavors of VPN:
 - PPTP, IPSec, L2TP over IPSec, SSL
- VPN Endpoint: Router or Server?
- How to manage user/passwords?

LEFT
40.5 U.S.
GALLONS
USABLE



RIGHT
40.5 U.S.
GALLONS
USABLE

OFF

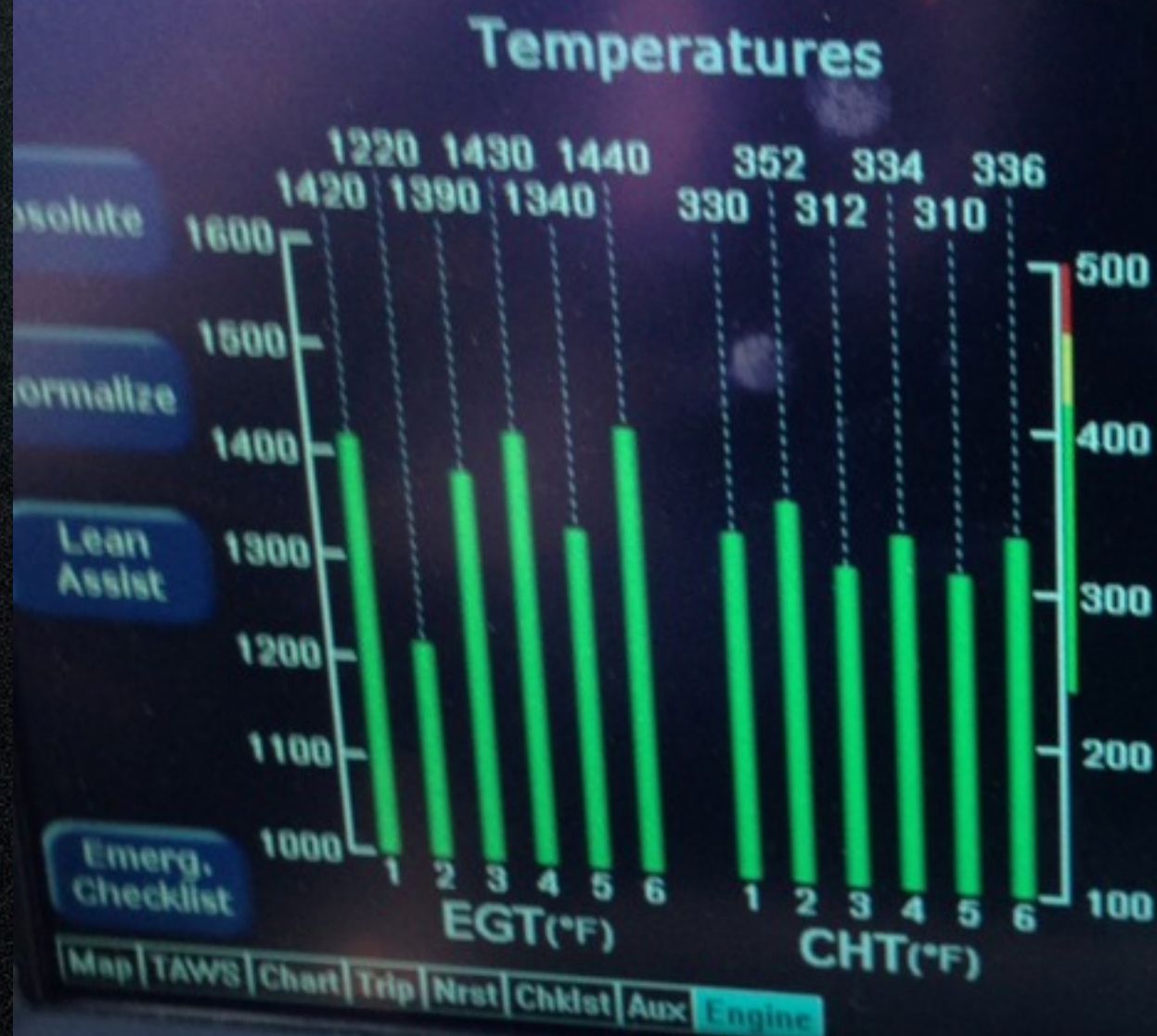
OFF

LIFT BUTTON FOR OFF POSITION

OIL DUE 647.8

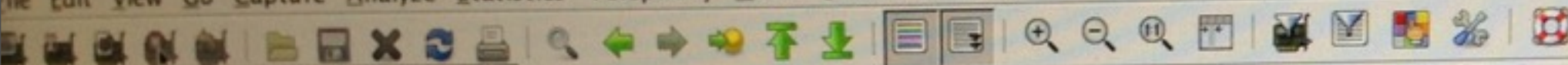
Troubleshooting

- Configure your laptop to be a syslog server
- Port mirroring & wireshark
- Joking around with the ISP



Choosing content filtering

- Configure your laptop to be a syslog server
- Lightspeed Systems
- iPrism



Filter: Stop the running live capture

Expression...

Clear

Apply

Save

Windows Clients

Mail out

My machine Src = n

No.	Time	Source	Destination	Protocol	Length	Info
8773	31.927377000	10.20.80.122	23.21.219.16	TLSv1	1514	Application Data, Application Data
8774	31.927380000	10.20.80.122	23.21.219.16	TLSv1	1514	Application Data, Application Data, Application Data
8775	31.927580000	23.21.219.16	10.20.80.122	TCP	66	https > 52890 [ACK] Seq=1 Ack=197636 Win=1177 Len=0 TSval=13897847
8776	31.939917000	10.20.80.12	192.168.19.0	SNMP	127	get-request 1.3.6.1.2.1.1.3.0 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.4.0 1.
8777	31.940022000	10.20.80.12	10.20.80.1	SNMP	316	get-next-request 1.3.6.1.2.1.2.2.1.10.3 1.3.6.1.2.1.2.2.1.16.3 1.3.6.
8778	31.940404000	10.20.80.1	10.20.80.12	SNMP	341	get-response 1.3.6.1.2.1.2.2.1.10.4 1.3.6.1.2.1.2.2.1.16.4 1.3.6.1.2.
8779	31.953391000	10.20.80.77	23.62.162.45	TCP	66	51922 > https [ACK] Seq=69957 Ack=631327 Win=129616 Len=0 TSval=4907
8780	31.953395000	23.62.162.45	10.20.80.77	TLSv1	1514	Application Data
8781	31.954410000	10.20.80.77	23.62.162.45	TCP	66	51922 > https [ACK] Seq=69957 Ack=632775 Win=131072 Len=0 TSval=4907
8782	31.954416000	23.62.162.45	10.20.80.77	TCP	1514	[TCP segment of a reassembled PDU]
8783	31.955585000	10.20.80.12	10.20.80.1	SNMP	316	get-next-request 1.3.6.1.2.1.2.2.1.10.4 1.3.6.1.2.1.2.2.1.16.4 1.3.6.
8784	31.955932000	10.20.80.1	10.20.80.12	SNMP	339	get-response 1.3.6.1.2.1.2.2.1.10.5 1.3.6.1.2.1.2.2.1.16.5 1.3.6.1.2.
8785	31.971024000	10.20.80.12	192.168.17.149	SNMP	127	get-request 1.3.6.1.2.1.1.3.0 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.4.0 1.
8786	31.975292000	10.20.80.122	23.21.219.16	TLSv1	1514	Application Data, Application Data, Application Data
8787	31.975295000	10.20.80.122	23.21.219.16	TLSv1	1514	Application Data, Application Data
8788	31.975577000	23.21.219.16	10.20.80.122	TCP	66	https > 52890 [ACK] Seq=1 Ack=200532 Win=1177 Len=0 TSval=13897895 TS
8789	31.977241000	10.20.80.65	198.147.175.225	ESP	126	ESP (SPI=0x9f6011f1)
8790	31.986412000	10.20.80.12	192.168.19.114	ICMP	62	Echo (ping) request id=0x9f52, seq=178/45568, ttl=64
8791	31.991972000	198.147.175.225	10.20.80.65	ESP	1358	ESP (SPI=0x07615253)
8792	32.002415000	10.20.80.77	23.62.162.45	TCP	66	51922 > https [ACK] Seq=69957 Ack=634223 Win=129616 Len=0 TSval=49072
8793	32.002601000	23.62.162.45	10.20.80.77	TCP	1514	[TCP segment of a reassembled PDU]
8794	32.003365000	10.20.80.77	23.62.162.45	TCP	66	51922 > https [ACK] Seq=69957 Ack=635671 Win=129616 Len=0 TSval=49072
8795	32.003486000	23.62.162.45	10.20.80.77	TLSv1	1514	Application Data
8796	32.003489000	23.62.162.45	10.20.80.77	TCP	1514	[TCP segment of a reassembled PDU]
8797	32.006392000	10.20.80.68	70.91.194.1	TCP	62	52115 > 61702 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
8798	32.008315000	10.20.80.167	138.237.49.161	TCP	62	49637 > us-srv [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM=1
8799	32.023412000	10.20.80.122	23.21.219.16	TLSv1	1514	Application Data, Application Data, Application Data
8800	32.023416000	10.20.80.122	23.21.219.16	TLSv1	1514	Application Data, Application Data, Application Data
8801	32.023600000	23.21.219.16	10.20.80.122	TCP	66	https > 52890 [ACK] Seq=1 Ack=203428 Win=1177 Len=0 TSval=13897943 TS

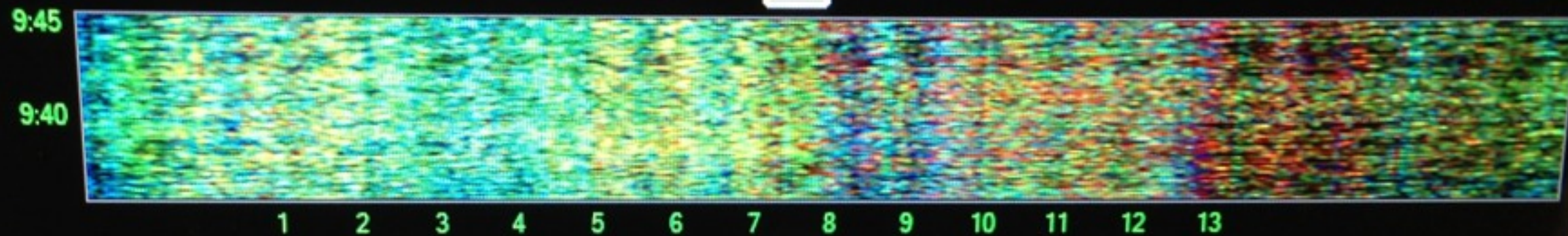
Frame 1635: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface 0
Ethernet II, Src: HewlettP_05:d2:74 (24:be:05:05:d2:74), Dst: Apple_14:3b:5b (b8:f6:b1:14:3b:5b)
Destination: Apple_14:3b:5b (b8:f6:b1:14:3b:5b)
Source: HewlettP_05:d2:74 (24:be:05:05:d2:74)
Type: IP (0x0800)

Internet Protocol Version 4, Src: 17.173.66.48 (17.173.66.48), Dst: 10.20.80.77 (10.20.80.77)

0000	b8 f6 b1 14 3b 5b 24 be	05 05 d2 74 08 00 45 00[S. ...t..E.
0010	05 dc af 23 40 00 40 06	d7 ba 11 ad 42 30 0a 14	...#@.80..
0020	50 4d 01 bb ca c6 f9 8b	10 34 30 07 b7 76 80 10	PM.....40..v..
0030	00 6c 60 91 00 00 01 01	08 0a 00 d3 a8 4b 1d 3f	.l'.....K.?
0040	68 b1 65 2e 63 6f 6d 82	18 70 31 39 2d 62 75 79	h.e.com. .p19-buy
0050	2e 69 74 75 6e 65 73 2e	61 70 70 6c 65 2e 63 6f	.itunes. apple.co
0060	6d 82 18 70 32 30 2d 62	75 79 2e 69 74 75 6e 65	m. p20-b uy.itune
0070	73 2e 61 70 70 6c 65 2e	63 6f 6d 82 18 70 32 31	s.apple. com. p21
0080	2d 62 75 79 2e 69 74 75	6e 65 73 2e 61 70 70 6c	-buy.itu nes.appl
0090	65 2e 63 6f 6d 82 18 70	32 32 2d 62 75 79 2e 69	e.com. p 22-buy.1
00a0	74 75 6e 65 73 2e 61 70	70 6c 65 2e 63 6f 6d 82	tunes.ap ple.com.
00b0	10 70 73 73 7d 67 75 70	70 60 7d 75 60 65 73 70	n23.buy itunes

Ready to load or capture

Packets: 8801



News Showcase Signatures Networks Table **Networks Graph** Channels Table % Utilization





MACTECH