Client C- Firebox Review

3/31/2021

Contents

Switches

There are no current switches that support proper microsegmentation strategies.

Firebox Location A-M200

Fireware 11.10.2.B484746

Fireware is extremely old. The Firebox needs a properly configured USB flash drive installed in the Firebox. The installed version of Fireware does not support any of the modern configurations and is missing all of the current security patches and bug fixes.

LAN IP for flat subnet: 192.168.3.1/24

Issues

DNS for Firebox using internal DC. The Firebox should never look internally for DNS. This is the DNS that the Firebox needs to function. Use of an internal DC causes serious latency issues and is not adding any value.

Germany is not able to manage the Firebox over WSM, but they should have that configured. Per client contact they are TeamViewer connecting to a server and then manage the Firebox instead going direct from a WSM server. The Firebox at Location A is being managed from the domain controller. It should not be managed this way. If Germany is going to manage the Firebox, it should be enrolled in a WSM server and proper network communications on both sides need to be setup to facilitate that.

WSM management traffic DOES NOT go over a BOVPN. It is certificate and WAN IP ACL restricted traffic on both sides.

It appears that no one is monitoring the Firebox because Windstream is down and no one knew about it. The SDWAN configuration is far from being effective. There is no detection in effect and routing table is a configuration that should not be used. Round-Robin with proper weights and controlled SDWAN actions per policy set is a much better configuration. No notifications are setup to facilitate anyone being able to monitor the SD WAN status or other alarm statuses on the device.

There is no requirement for a technical person to be physically present in order to execute a recovery. Proper preparation, photographs, and procedures eliminate the requirement that a technical person be

physically present for a recovery. The organization may wish to invest in a FireCluster scenario. We strongly recommend 4-hour hardware warranty contracts on the Fireboxes even with FireCluster. We have performed many recoveries remotely in the past when the proper prerequisites existed. Physical presence requirements should not be a reason to delay upgrading Fireware. Instead, a proper Firebox resiliency design and all of the prerequisites for configuration restore/recovery must be in place.

Furthermore, what is the plan for a hardware failure? If the Firebox hardware dies, this should not require a physical onsite visit by any technical personnel. The onsite staff should be able to take out the defective Firebox and rack the new Firebox and then be smart hands to connect a laptop to the new Firebox to execute the remote recovery. We do these functions regularly and no onsite visits are required. We have talked many very non-technical people through what to do and it has worked each time.

The M200 is end of support December 2022. My current recommendation based upon the information I have about the current Location A network and what it should be is that a M390 with TSS should be installed. I would not copy over the configuration from the M200. I would start from one of our templates and then add the things into the configuration which are actually still needed. It would take much longer to remediate the current configuration than to start with one of our configurations. I would take this approach in the realm that QPC is going to be involved in the ongoing management of the Firebox. If the support model is planned to be different, then another approach should be discussed. WatchGuard support is not capable of supporting the high security configurations that we use. WatchGuard support is break/fix, not strategic security engineering.

I would remove the Erbs certificate. It appears that the Firebox is missing a certificate that protects login credentials to the website. This needs to be corrected. We usually put a wildcard certificate on the appliance that is associated with a FQDN which is equally resolvable internally and externally. This way logins to the appliance are protected as well as interactions with it in general. Having a proper viable certificate on the Firebox is also REQUIRED for the VPN.

Please understand that right now every time one of your users does SSL VPN to that Firebox, the Active Directory credentials of that user is not only transmitted in cleartext across the internet, but it is also transmitted in cleartext inside your network to the domain controller. This is an unacceptable security risk condition.

Firebox needs a USB flash drive attached to it. Triple mode backups need to be made and occurring.

There are many settings that are missing or just misconfigured inside the M200.

The renewal that Client purchased in November 2021 was never applied. Someone needs to activate that on the M200 in the WatchGuard website account where the M200 is registered. Obtain the feature key and install that in the firebox. We should have conversations about where that Firebox is registered and in what tenant because if you want to solve the SSL VPN issue, that Firebox should be migrated to a subscriber account where we can put the MFA licensing and provide proper support to you for that solution.

The phone system is not properly isolated. It is on an optional network and that should not be configured as an optional network. It should be custom. Conversations with the people who manage the phone system need to be had to determine exactly what ingress/egress policies are required for the phone system. The current configuration would not pass a vulnerability assessment.

The BOVPN is wide open. Furthermore, the traffic is not even being logged. The SSL VPN traffic is not being logged. And the SSL VPN policy is wide open.

Those three policies should be disabled and the traffic for SSL VPN and BOVPN must be vastly more tightly restricted and controlled.

DNS traffic egressing should be proxied. It is not being proxied currently. Furthermore, no devices on Trusted should be able to access external DNS servers. For trusted type VLANs, those devices must send their DNS requests to authorized domain controllers. Only domain controllers should be allowed to egress TCP/UDP 53 to authorized and restricted DNSWatch DNS servers and the traffic should be proxied. Custom security zone VLAN should either be configured to use AD DS DNS if they are domain joined assets, or they should be in a SEPARATE DNS proxy and only allowed to egress DNS packets to DNSWatch servers.

This configuration is fully open to data exfiltration over the DNS channel with zero visibility into that threat vector.

Regarding policies 3,4,6,7,16,17 IP addresses should never be used in policies like that. Aliases should be created. The aliases appear in the policies. IP addresses are put into Aliases. Network documentation must exist which specifies exactly what these IP addresses are and what the policy is supposed to do or what functionality it is supposed to facilitate. Use of IP addresses instead of aliases makes the policy set more difficult to audit and diminishes the value of the policy-based documentation. It also increases the probability of human failure because when an IP address needs to be changed, it must be changed across all the policies where that information was used instead of a single alias. Aliases have descriptions. The descriptions should be used with the level of detail to make auditing configurations and understanding what these assets are very easy.

The Outgoing policy must be disabled. Preferably outright deleted. Proper egress filtration must be setup.

Egress traffic is not being secured or proxied or restricted in any way in this configuration. There is no vulnerability assessment that this configuration would pass. Proxy certificates are probably not being deployed to workstations via AD GPO. This should be setup. I would also want to see the GPOs for all the browsers used in the organization that will control the proxy and certificate settings. I did not look at those, but I suspect those are missing.

VLANs are not being used. The environment does not have the structure or configuration to facilitate required microsegmentation. All cybersecurity insurance requires proper network segmentation. This configuration does not deliver a yes on that requirement. Domain controllers must be in their own dedicated and isolated VLAN. Proper policies are required for DC-to-DC communications with aliases being used. Proper policies to allow AD DS domain-joined assets to communicate with the DCs on only the ports and protocols required, no more. DCs should be in a custom security zone VLAN.

By not using VLANs, the Firebox is significantly less flexible in its configuration. By not using the Firebox as the core router for many subnets, the organization is not allowing the Firebox to secure, inspect, log, monitor, and secure inter and intra-VLAN packets.

Copiers and printers should be on a Printers VLAN with ACL restrictions. This should also be a custom security zone.

I do not see evidence of supply chain risk management in this configuration. An inventory of the assets at the facility would be helpful. For example, if there are any surveillance cameras or VMS (video management server) these assets must be on a custom security zone surveillance VLAN. I do not see any VLAN for HVAC equipment, electrical metering equipment, door controllers, or any IoT systems which are typical in manufacturing environments. An inventory of the assets at the environment would probably reveal thermostats, HVAC controllers and other assets that have no business whatsoever being on the same VLAN with AD DS joined assets.

File services and other services should not be hosted on the domain controller. WatchGuard SSO Gateway and AuthPoint server can be installed on domain controllers in environments that do not employ AD DS account logon restrictions for SSL VPN users. In more hardened environments, that would require AuthPoint services to be installed on a non-DC member server.

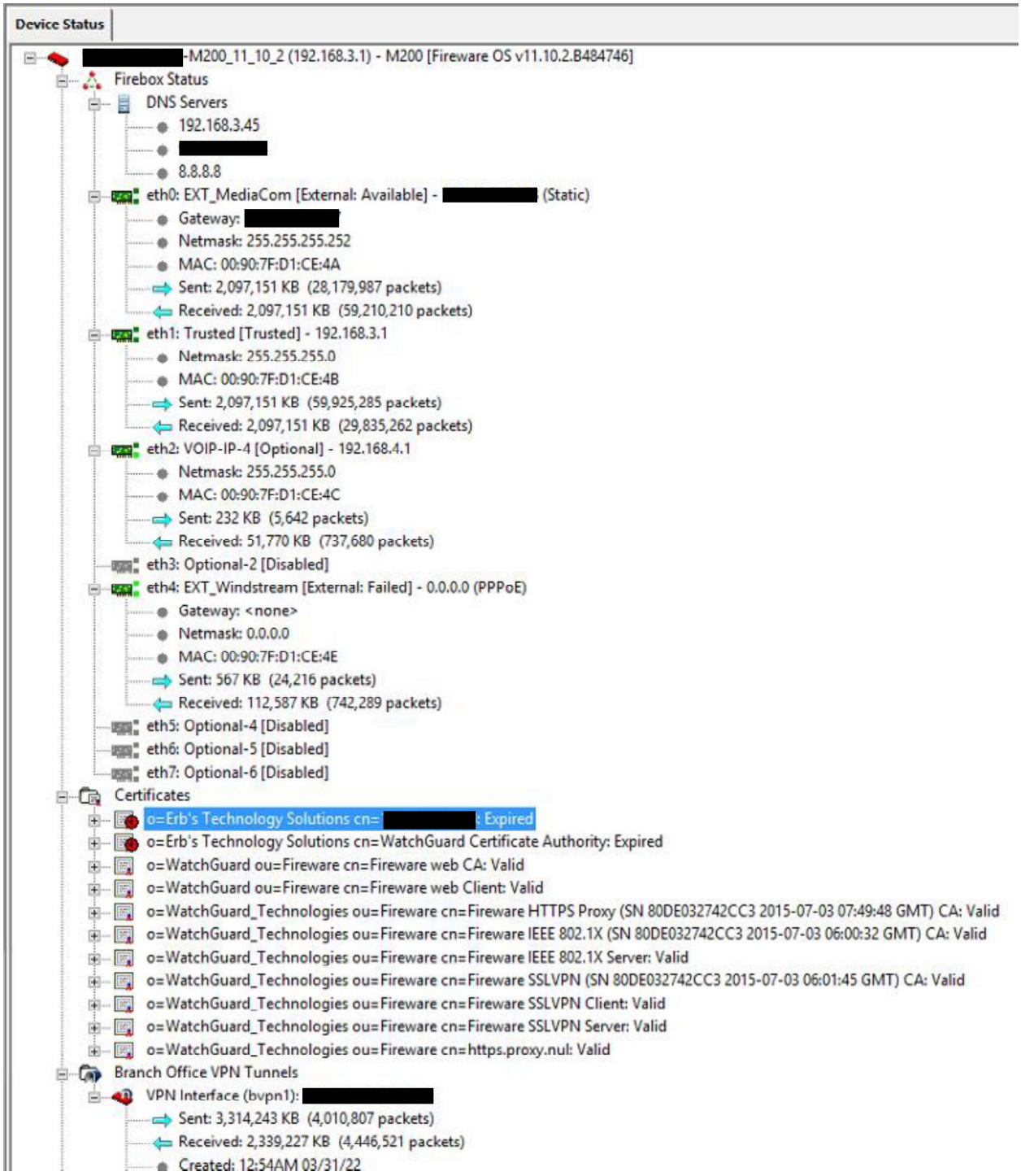
Old server operating system should not be used anymore for any DCs. LDAPS must be setup between Firebox and DCs. Old server operating systems less than 2016 adversely affect the ability to properly secure ADDS.

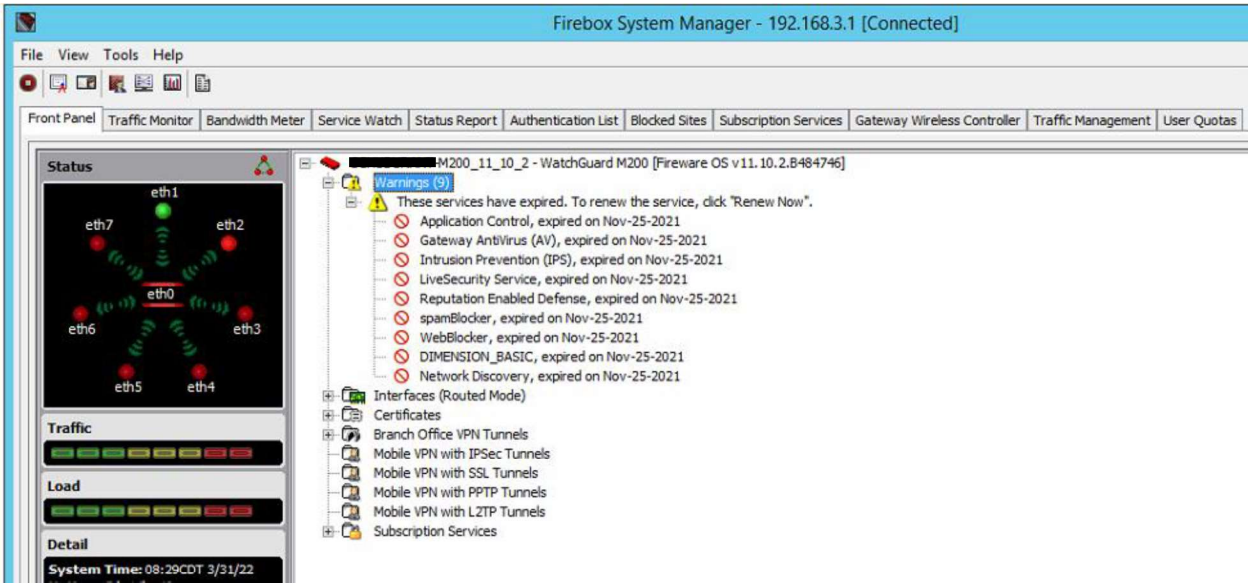
There is no SSO configuration being used, and it should be used.

The Firebox is not sending data to a Dimension server or WatchGuard Cloud. Therefore, there is no alarm notification mechanism or diagnostic mechanism in place. Overall, the configuration is completely lacking in proper logging levels.

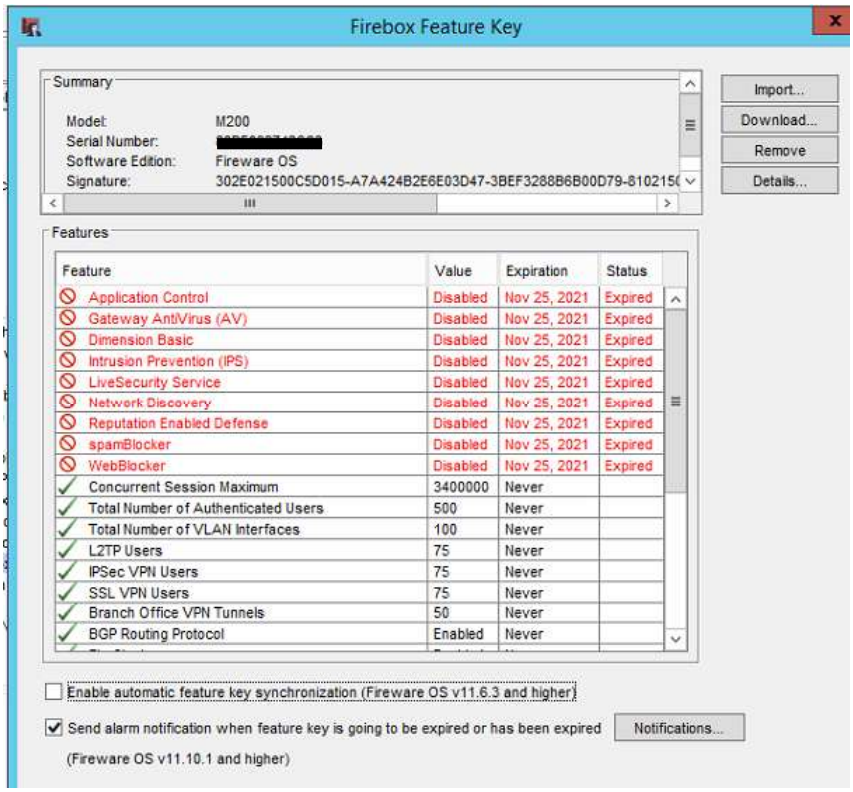
A mandatory security and cybersecurity insurance requirement is proper logging and visibility of traffic. A perimeter only strategy does not facilitate an outcome of visibility or proper network layer security. Very few of the policies have logging configured, but without the Firebox configured to send the logs somewhere, no log data whatsoever is being collected. This makes diagnostics and compliance reporting next to impossible.

Automatic feature key synchronization should be enabled.

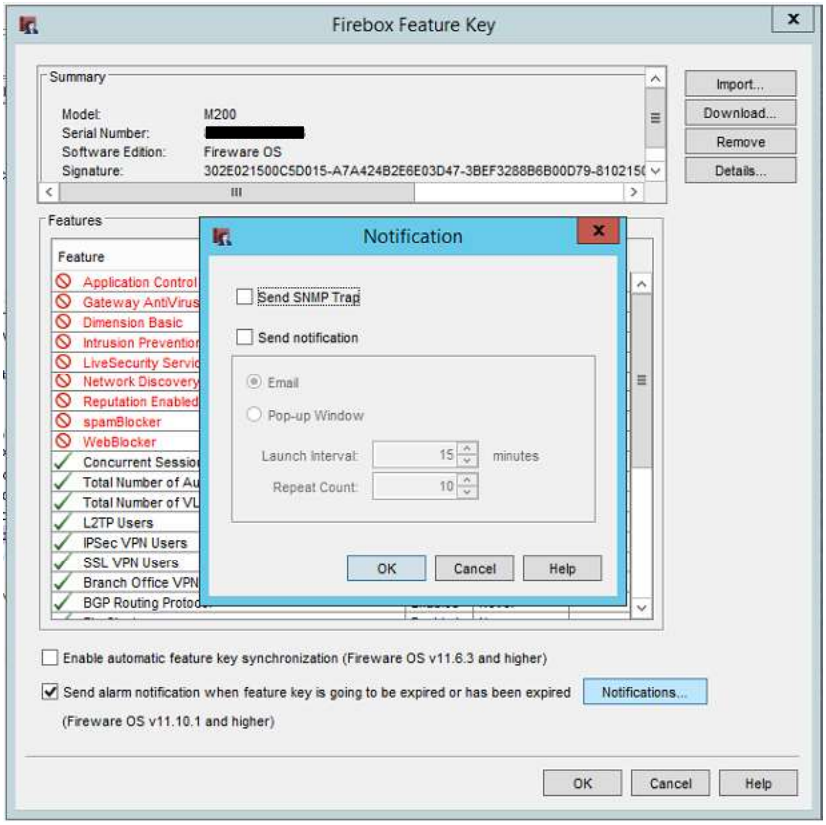

Device Status
[redacted]-M200_11_10_2 (192.168.3.1) - M200 [Fireware OS v11.10.2.B484746]
Firebox Status
DNS Servers
192.168.3.45
[redacted]
8.8.8.8
eth0: EXT_MediaCom [External: Available] - [redacted] (Static)
Gateway: [redacted]
Netmask: 255.255.255.252
MAC: 00:90:7F:D1:CE:4A
Sent: 2,097,151 KB (28,179,987 packets)
Received: 2,097,151 KB (59,210,210 packets)
eth1: Trusted [Trusted] - 192.168.3.1
Netmask: 255.255.255.0
MAC: 00:90:7F:D1:CE:4B
Sent: 2,097,151 KB (59,925,285 packets)
Received: 2,097,151 KB (29,835,262 packets)
eth2: VOIP-IP-4 [Optional] - 192.168.4.1
Netmask: 255.255.255.0
MAC: 00:90:7F:D1:CE:4C
Sent: 232 KB (5,642 packets)
Received: 51,770 KB (737,680 packets)
eth3: Optional-2 [Disabled]
eth4: EXT_Windstream [External: Failed] - 0.0.0.0 (PPPoE)
Gateway: <none>
Netmask: 0.0.0.0
MAC: 00:90:7F:D1:CE:4E
Sent: 567 KB (24,216 packets)
Received: 112,587 KB (742,289 packets)
eth5: Optional-4 [Disabled]
eth6: Optional-5 [Disabled]
eth7: Optional-6 [Disabled]
Certificates
o=Erb's Technology Solutions cn=[redacted]: Expired
o=Erb's Technology Solutions cn=WatchGuard Certificate Authority: Expired
o=WatchGuard ou=Fireware cn=Fireware web CA: Valid
o=WatchGuard ou=Fireware cn=Fireware web Client: Valid
o=WatchGuard_Technologies ou=Fireware cn=Fireware HTTPS Proxy (SN 80DE032742CC3 2015-07-03 07:49:48 GMT) CA: Valid
o=WatchGuard_Technologies ou=Fireware cn=Fireware IEEE 802.1X (SN 80DE032742CC3 2015-07-03 06:00:32 GMT) CA: Valid
o=WatchGuard_Technologies ou=Fireware cn=Fireware IEEE 802.1X Server: Valid
o=WatchGuard_Technologies ou=Fireware cn=Fireware SSLVPN (SN 80DE032742CC3 2015-07-03 06:01:45 GMT) CA: Valid
o=WatchGuard_Technologies ou=Fireware cn=Fireware SSLVPN Client: Valid
o=WatchGuard_Technologies ou=Fireware cn=Fireware SSLVPN Server: Valid
o=WatchGuard_Technologies ou=Fireware cn=https.proxy.nul: Valid
Branch Office VPN Tunnels
VPN Interface (bvpn1): [redacted]
Sent: 3,314,243 KB (4,010,807 packets)
Received: 2,339,227 KB (4,446,521 packets)
Created: 12:54AM 03/31/22



No one applied the license key to the Firebox which was purchased in 2021.



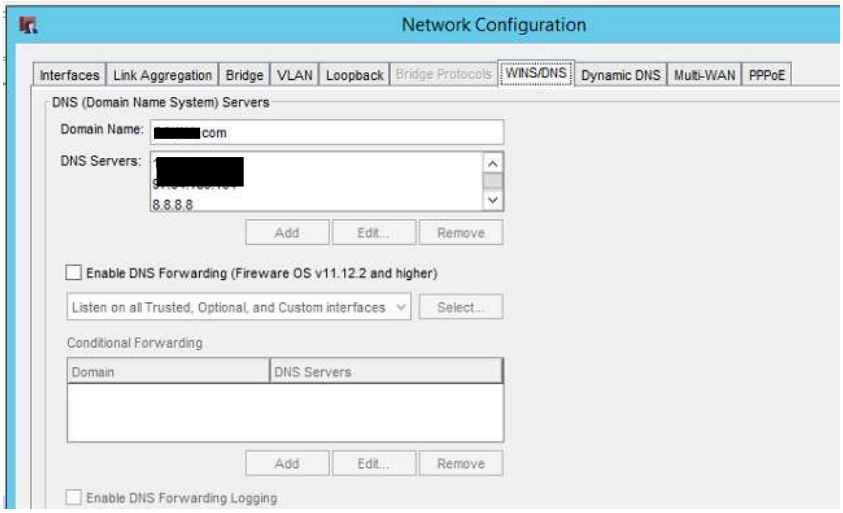
Notifications are not enabled.



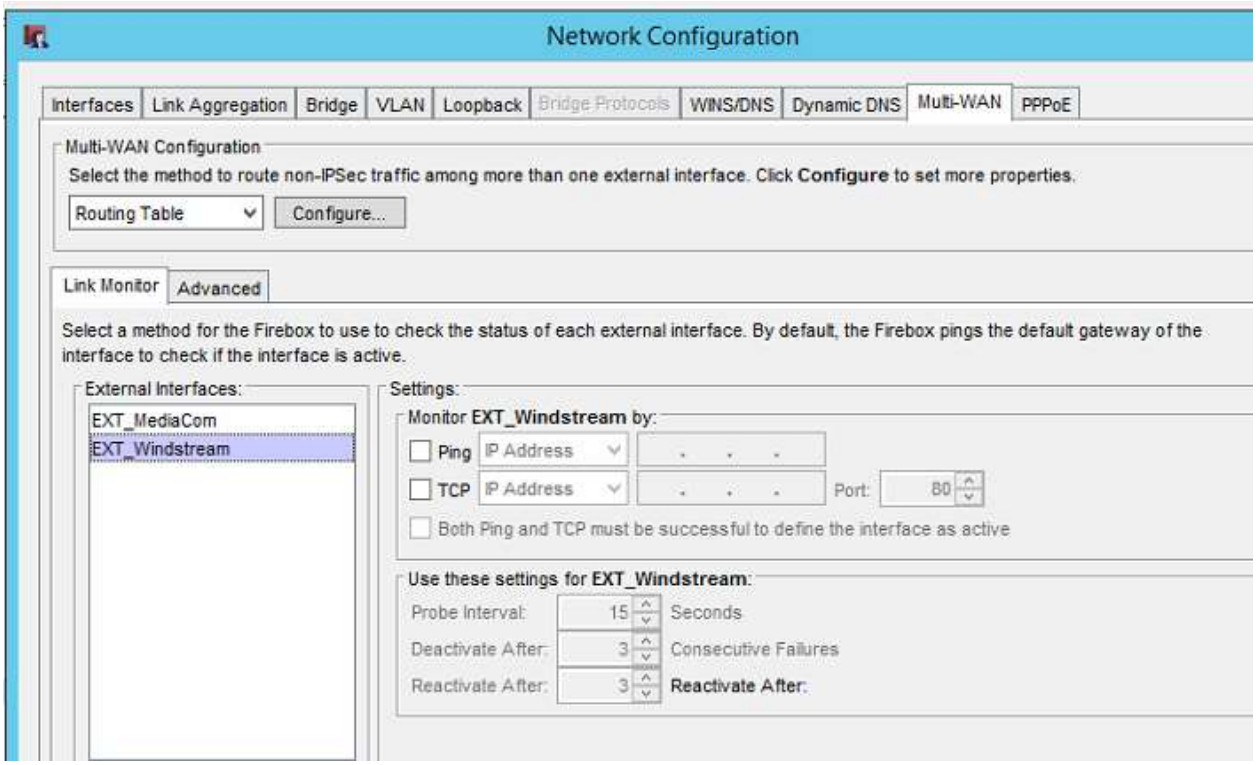
Internal DNS should never be used for Firebox DNS. ISP-specific DNS servers should never be used for Firebox DNS. Only servers such as 1.1.1.1, 1.0.0.1, 8.8.8.8 should ever be used for Firebox DNS.

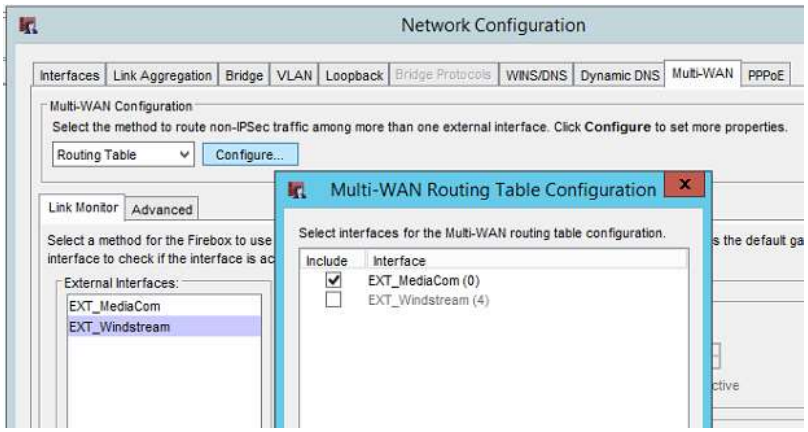
DNS Watch is not configured.

The AD DS domain name should not be used in the network configuration for the Firebox.

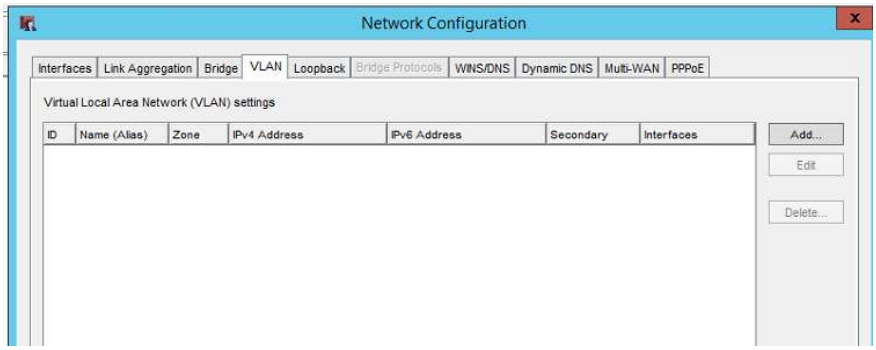


SDWAN configuration is not configured in such a way that it will work effectively.





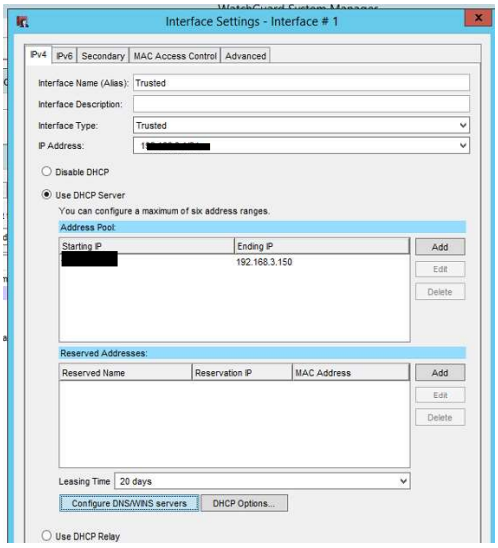
No VLANs.



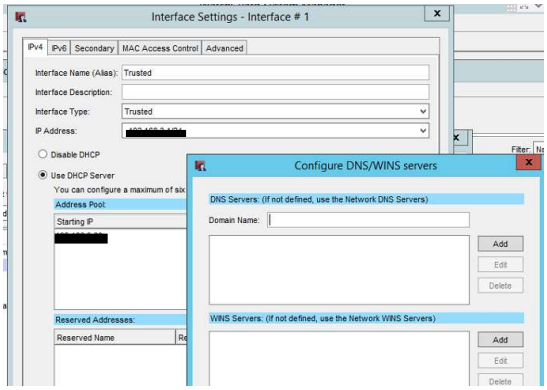
There are no proper DNS or DHCP option configurations in this Firebox to support an ADDS environment.

If any of the servers have management interfaces, there is nothing in this configuration that would support properly isolating them. Server management interfaces must be on a custom security zone VLAN with strict supply chain risk management restrictions as well as tight ACLs even for east-west traffic, full logging, full IPS, and application control.

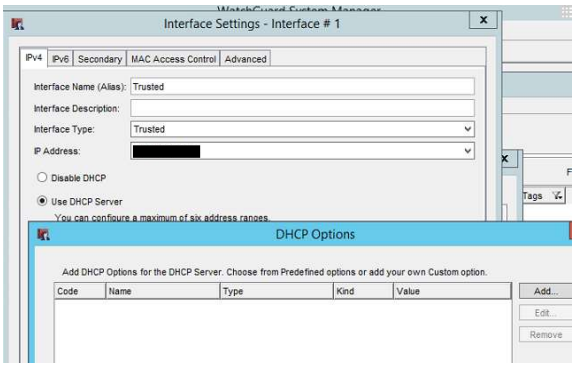
The same is true for management interfaces for switches.



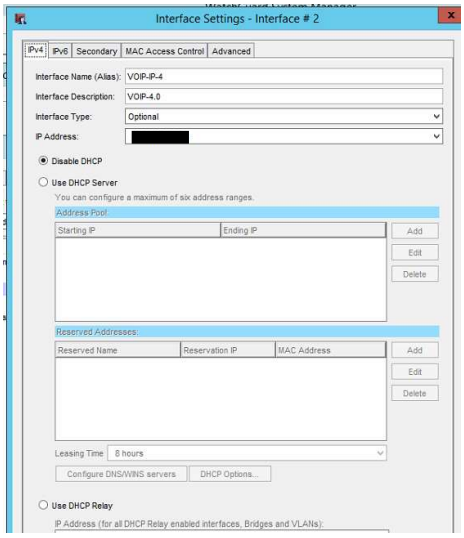
Proper DNS not being provided to ADDS joined assets on this VLAN.



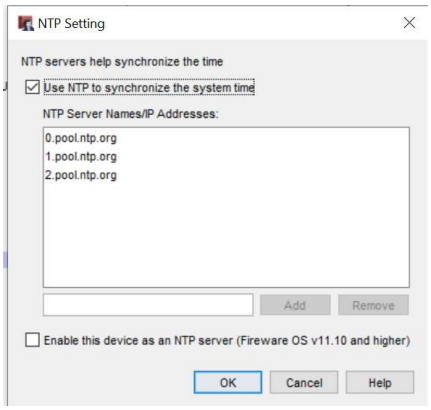
No DHCP options to support ADDS properly for domain joined assets.



Phone VLAN should not be optional. It should be custom. Many other hardening measures around traffic to/from that subnet should be in place.

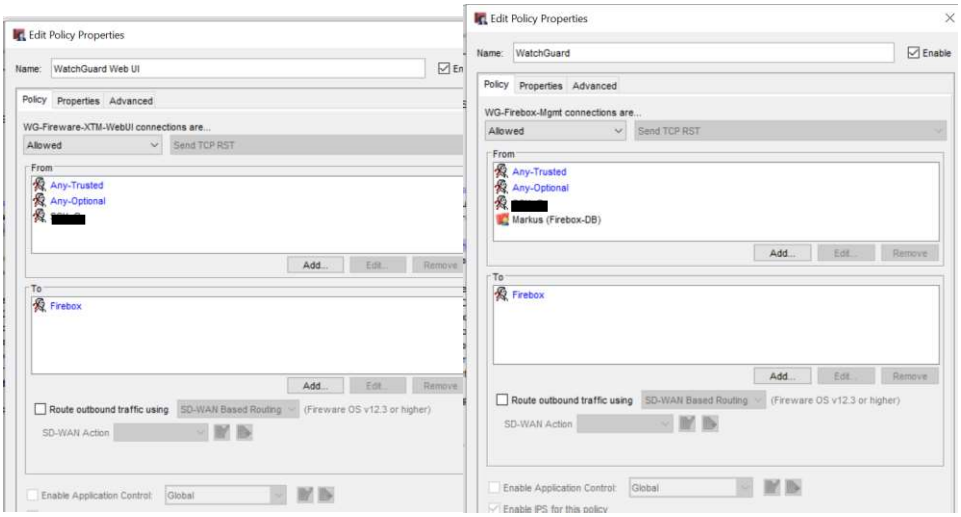


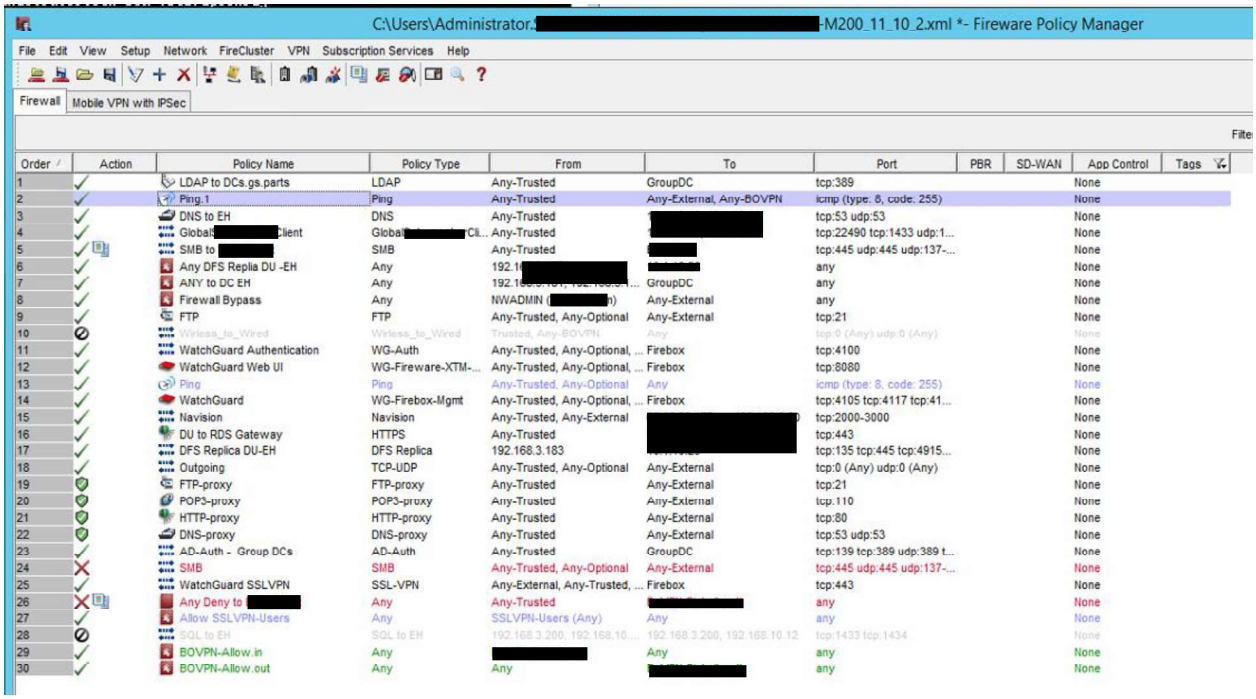
NTP is not configured properly here or in policies or DHCP options.



The Firebox management interface should not be this open. This configuration allows assets on the phone network to connect to the management interface of the Firebox. Any-Trusted should NOT be used. Firebox management should be restricted to the alias which is the static WAN IPs of the management server and authorized management planes, and then premise PAWs (privileged admin workstations) which should also be on a custom security zone PAW VLAN. The Firebox should not be manageable from a domain controller VLAN or a server VLAN, and certainly not from a VLAN where general PCs exist.

Logging is not enabled for the management policies. This must be corrected to have visibility and compliance. The WSM server should have a daily compliance report for all changes made to Fireboxes. That report should be reviewed by the compliance officer daily and those reports should be sent to the GRC in a compliance document repository with 180 day retention at a minimum.



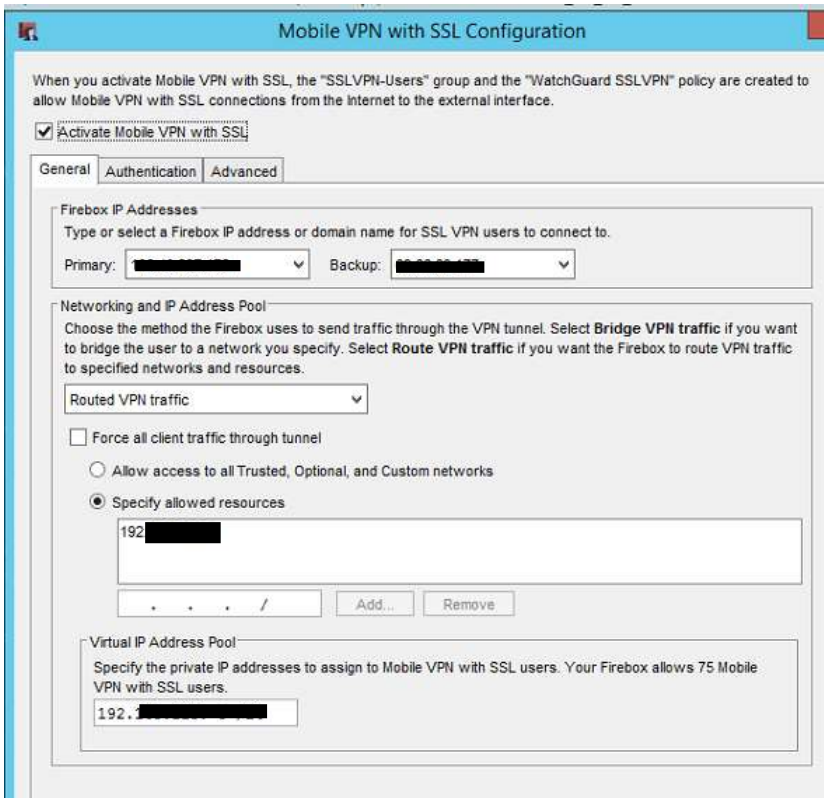


Order	Action	Policy Name	Policy Type	From	To	Port	PBR	SD-WAN	App Control	Tags
1	✓	LDAP to DCs.gs.parts	LDAP	Any-Trusted	GroupDC	tcp:389			None	
2	✓	Ping.1	Ping	Any-Trusted	Any-External, Any-BOVPN	icmp (type: 8, code: 255)			None	
3	✓	DNS to EH	DNS	Any-Trusted	[redacted]	tcp:53 udp:53			None	
4	✓	Global[redacted]lient	Global[redacted]Cli...	Any-Trusted		tcp:22490 tcp:1433 udp:1...			None	
5	✓	SMB to [redacted]	SMB	Any-Trusted	[redacted]	tcp:445 udp:445 udp:137-...			None	
6	✓	Any DFS Replia DU -EH	Any	192.1[redacted]	[redacted]	any			None	
7	✓	ANY to DC EH	Any	192.[redacted]...	GroupDC	any			None	
8	✓	Firewall Bypass	Any	NWADMIN ([redacted]n)	Any-External	any			None	
9	✓	FTP	FTP	Any-Trusted, Any-Optional	Any-External	tcp:21			None	
10	⊘	Wirless_to_Wired	Wirless_to_Wired	Trusted, Any-BOVPN	Any	tcp:0 (Any) udp:0 (Any)			None	
11	✓	WatchGuard Authentication	WG-Auth	Any-Trusted, Any-Optional, ...	Firebox	tcp:4100			None	
12	✓	WatchGuard Web UI	WG-Fireware-XTM-...	Any-Trusted, Any-Optional, ...	Firebox	tcp:8080			None	
13	✓	Ping	Ping	Any-Trusted, Any-Optional	Any	icmp (type: 8, code: 255)			None	
14	✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-Optional, ...	Firebox	tcp:4105 tcp:4117 tcp:41...			None	
15	✓	Navision	Navision	Any-Trusted, Any-External	[redacted]	tcp:2000-3000			None	
16	✓	DU to RDS Gateway	HTTPS	Any-Trusted		tcp:443			None	
17	✓	DFS Replica DU-EH	DFS Replica	192.168.3.183		tcp:135 tcp:445 tcp:4915...			None	
18	✓	Outgoing	TCP-UDP	Any-Trusted, Any-Optional	Any-External	tcp:0 (Any) udp:0 (Any)			None	
19	✓	FTP-proxy	FTP-proxy	Any-Trusted	Any-External	tcp:21			None	
20	✓	POP3-proxy	POP3-proxy	Any-Trusted	Any-External	tcp:110			None	
21	✓	HTTP-proxy	HTTP-proxy	Any-Trusted	Any-External	tcp:80			None	
22	✓	DNS-proxy	DNS-proxy	Any-Trusted	Any-External	tcp:53 udp:53			None	
23	✓	AD-Auth - Group DCs	AD-Auth	Any-Trusted	GroupDC	tcp:139 tcp:389 udp:389 t...			None	
24	✗	SMB	SMB	Any-Trusted, Any-Optional	Any-External	tcp:445 udp:445 udp:137-...			None	
25	✓	WatchGuard SSLVPN	SSL-VPN	Any-External, Any-Trusted, ...	Firebox	tcp:443			None	
26	✗	Any Deny to [redacted]	Any	Any-Trusted	[redacted]	any			None	
27	✓	Allow SSLVPN-Users	Any	SSLVPN-Users (Any)	Any	any			None	
28	⊘	SQL to EH	SQL to EH	192.168.3.200, 192.168.10....	192.168.3.200, 192.168.10.12	tcp:1433 tcp:1434			None	
29	✓	BOVPN-Allow.in	Any	[redacted]	Any	any			None	
30	✓	BOVPN-Allow.out	Any	Any	[redacted]	any			None	

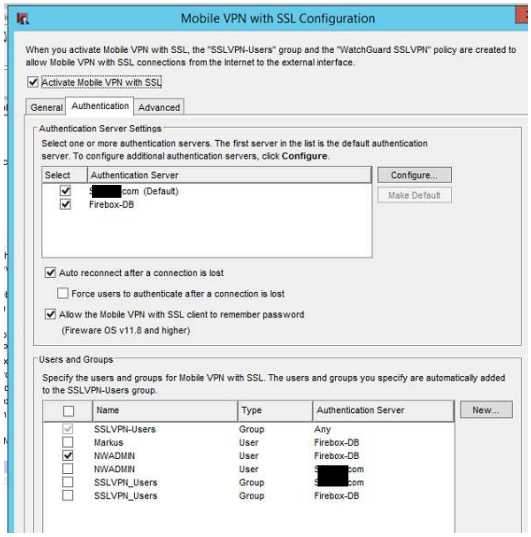
Policy 8 is highly problematic. It is way too wide open and no logging.

FTP should be proxied, but the built-in proxy policy cannot be used because it does not support the full FTP proxy channels required. Right now the environment is open to full data exfiltration over FTP as it is not restricted and not logged.

Backup VPN connection is irrelevant when SD WAN is not working and not configured properly. The VPN is incorrectly configured where it is not a force tunnel and the policies are not restricted or logged.

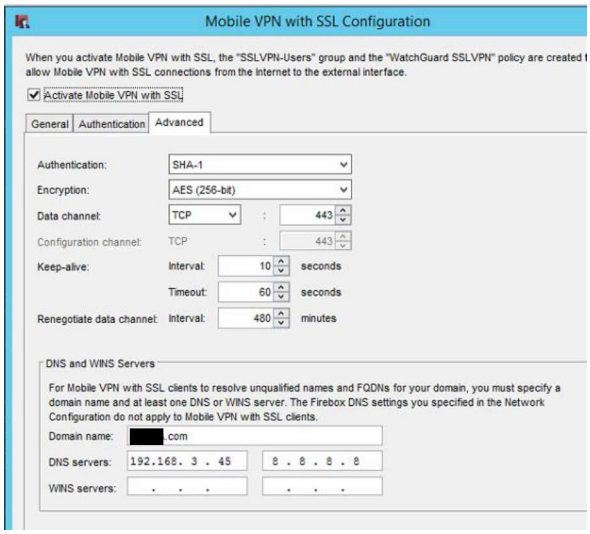


This configuration indicates that the primary SSL VPN authentication database is Active Directory. Yet the current configuration is extremely insecure allowing the transmission of usernames and passwords in cleartext.

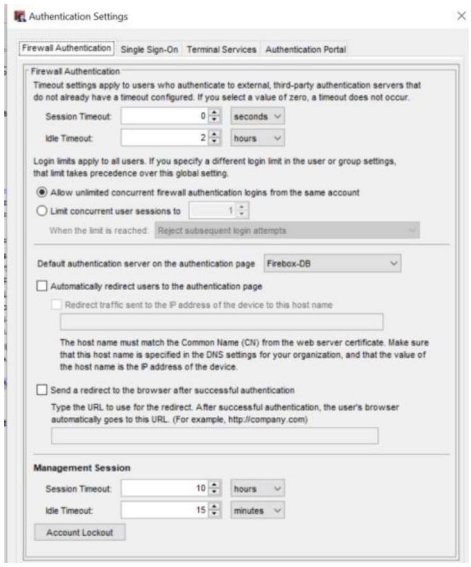


8.8.8.8 is not a DNS server that should be provided to a SSL VPN client. It is not a DNS server that hosts DNS records authoritative for client website.

SHA1 was officially deprecated in 2011. This configuration does not pass basic security standards.



Overall Firewall authentication session timeout is disabled. This is a very insecure configuration. Users should not be allowed to remain indefinitely connected. It is better to use an eight or ten hour session timeout with an idle timeout of one to two hours.



LDAPS is not being used and there is no redundancy in this authentication. Because LDAPS is not being used, that suggests to me that the environment is missing an ADDS enterprise root CA, there is no LDAP channel binding and signing, old server technology is being used, and the AD DS GPO configurations are weak meaning not in a security hardened state. In March 2020, security defaults were strongly recommended to be changed by the US Federal Government as well as Microsoft. QPC switched all our clients to LDAPS at that time if they were not already using full LDAPS enforcement. Without the ADDS environment being remediated, you cannot enable LDAPS. If you do not have LDAPS communications working properly, you will not get SSL VPN MFA to work properly. Regardless, not using LDAPS is a significant security vulnerability.

Adaptive Defense 360 is not installed on server. No EPP on server at all. We currently use AD360 in a hardened state on around 200 servers without issue. Many of those are domain controllers, SQL servers, Exchange servers, web servers, application servers, and file servers. Client contact mentioned you were having problems with AD360 on servers so you are not using it on servers. Let's have a discussion about settings so that you can get EPP deployed to the servers.

Firebox DB accounts have no lockout restrictions or case sensitivity.

Summary

Cybersecurity insurance deficiencies are seen throughout this configuration. The current configuration does not put the organization in a strong position to detect or defeat malicious activity. The configuration is not defensible from an audit, vulnerability management, or cybersecurity position.

Everything can be fixed. Client contact received information from cybersecurity insurance that gaps must be resolved before insurance renewal period. It is going to be a sprint to resolve those issues. I strongly suggest engaging and getting those issues corrected as quickly as possible. Simply looking at the requirement for MFA for SSL VPN, getting that corrected and secured properly before the insurance renewal period is going to be a sprint. There is a great deal of work to do there considering the lack of prerequisites which are in place.

If you ask how much time it will take, that is highly contingent upon what you want to fix. I would fix all of it, but that is a considerable amount of time. I don't know what your short or long term goals are. I also see some sprint issues in the current support model. We can talk about these verbally in a meeting.