

## Client C- Firebox Review

### Contents

| Switches                | 1 |
|-------------------------|---|
| Firebox Location A-M200 | 1 |
| Issues                  | 1 |
| Summary                 |   |

### 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 |  |
|---------------|--|
| E             | -M200_11_10_2 (192.168.3.1) - M200 [Fireware OS v11.10.2.B484746]  |
| i 🙏           | Firebox Status   |
| <u> </u>      | DNS Servers  |
|               | • 192.168.3.45   |
|               |  |
|               |  |
| <b> </b>      | eth0: EXT_MediaCom [External: Available] - Static (Static)   |
|               | Gateway:   |
|               | • Netmask: 255.255.255.252   |
|               | MAC: 00:90:7F:D1:CE:4A   |
|               | 📥 Sent: 2,097,151 KB (28,179,987 packets)  |
|               |  |
| <u> </u>      | eth1: Trusted [Trusted] - 192.168.3.1  |
|               | Wetmask: 255.255.255.0   |
|               | MAC: 00:90:7F:D1:CE:4B   |
|               |  |
|               | Received: 2,097,151 KB (29,835,262 packets)  |
| <b> </b>      | and the state of t |
|               | 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)  |
|               | ब्रह्म" eth3: Optional-2 [Disabled]  |
| <u> </u>      | eth4: EXT_Windstream [External: Failed] - 0.0.0.0 (PPPoE)  |
|               | Gateway: <none></none>   |
|               | • Netmask: 0.0.0.0   |
|               | MAC: 00:90:7F:D1:CE:4E   |
|               | Sent: 50/ KB (24,210 packets)  |
|               | Received: 112,587 KB (742,289 packets)   |
|               | The second  |
|               | main the Optional-S [Disabled]   |
|               | mm eth/: Optional-o [Disabled]   |
|               |  |
|               | O=Erb's Technology Solutions cn=     Cexpired     Cexpired   |
|               | o-Erb's Technology Solutions ch= watchouard Certificate Authonity: Expired   |
|               | o-WatchGuard ou-Fireware ch-Fireware web CA, valid   |
|               | o = WatchGuard Out - Neware ch = Neware web Client, Valid     o = WatchGuard Technologies ou = Fireware web Client, Valid     o = WatchGuard Technologies ou = Fireware ch = Fireware HTTPS Prove (SN 20DE022742CC3 2015-07-02 07:40:42 GMT) CA: 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 (Set object) Let of object and the other of the other of the other of the other ot      |
|               | 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 (bypn1):   |
|               | Sent: 3.314,243 KB (4.010.807 packets)   |
|               |  |
|               | Created: 12:54AM 03/31/22  |





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



| Summary             |                                |                   |              |          | ^         | Import   |
|---------------------|--------------------------------|-------------------|--------------|----------|-----------|----------|
| Model               | M200                           |                   |              |          | =         | Download |
| Serial Number:      | 00050007/0000                  |                   |              |          | 0.77      | Demouro  |
| Software Edition:   | Fireware OS                    |                   |              |          |           | Remove   |
| Signature:          | 302E021500C5D015-A7A           | 424B2E6E03D47-3   | BEF3288B6B00 | D79-8102 | 150 ~     | Details  |
| <                   | ш                              | 10                |              |          | >         |          |
| Features            |                                |                   |              |          |           |          |
| Feature             |                                | Value             | Expiration   | Status   |           |          |
| Application Con     | trol                           | Disabled          | Nav 25, 2021 | Expired  |           |          |
| Q Gateway AntiV     | inus (AV)                      | Disabled          | Nov 25, 2021 | Expired  | -         |          |
| Q Dimension Basic   |                                | Disabled          | Nov 25, 2021 | Expired  |           |          |
| Q Intrusion Preven  | tion (IPS)                     | Disabled          | Nov 25, 2021 | Expired  |           |          |
| Q LiveSecurity Se   | rvice                          | Disabled          | Nov 25, 2021 | Expired  |           |          |
| Network Discov      | ery                            | Disabled          | Nov 25, 2021 | Expired  | =         |          |
| S Reputation Enab   | led Defense                    | Disabled          | Nov 25, 2021 | Expired  |           |          |
| SpamBlocker         | for the second second          | Disabled          | Nov 25, 2021 | Expired  | 1         |          |
| WebBlocker          |                                | Disabled          | Nov 25, 2021 | Expired  | 1         |          |
| ✓ Concurrent Ses    | sion Maximum                   | 3400000           | Never        | 1        |           |          |
| ✓ Total Number of   | Authenticated Users            | 500               | Never        |          |           |          |
| ✓ Total Number of   | VLAN Interfaces                | 100               | Never        | 8 8      |           |          |
| ✓ L2TP Users        |                                | 75                | Never        |          |           |          |
| V IPSec VPN User    | s                              | 75                | Never        |          |           |          |
| SSL VPN Users       |                                | 75                | Never        |          |           |          |
| ✓ Branch Office \   | /PN Tunnels                    | 50                | Never        |          |           |          |
| BGP Routing Pro     | otocol                         | Enabled           | Never        |          | ~         |          |
| Enable automatic fe | eature key synchronization (Fi | reware OS v11.6.3 | and higher)  | d Noti   | fications |          |

### Notifications are not enabled.

| Summary                                    |                 |   | ^             | Import   |
|--|-----------------|---|---------------|----------|
| Model:                                     | M200            |   | ≡             | Download |
| Serial Number:<br>Software Edition:        | Fireware OS     |   |               | Remove   |
| Signature:                                 | 302E021500C     | 5D015-A7A424B2E6E03D47-3BEF3288B6B00D7  | 9-8102150 🗸   | Details  |
| <  | Ш               |   | >             |          |
| Features                                   |                 |   | Y             |          |
| Feature                                    | 10              | Notification  |               |          |
| Application Contro                         | 4               |   |               |          |
| Gateway AntiViru                           | s Send          | SNMP Trap   | a name        |          |
| O Dimension Basic                          |                 |   |               |          |
| O Intrusion Preventio                      | In Send         | notification  |               |          |
| LiveSecurity Serv                          |                 | -1  | - =           |          |
| Reputation Enable                          | a en a          | 28  | -             |          |
| SpamBlocker                                | O Pop           | i-up Window   |               |          |
| WebBlocker                                 |                 |   |               |          |
| Concurrent Sessio                          | Laur            | nch Interval. 15 👷 minutes  |               |          |
| ✓ Total Number of A                        | u Re            | peat Count 10   |               |          |
| ✓ Total Number of V                        | 1               |   |               |          |
| ✓ L2TP Users                               | , L             |   |               |          |
| IPSec VPN Users                            |                 | 10 March 10 |               |          |
| SSL VPN Users                              |                 | OK Cancel Help  |               |          |
| ✓ Branch Office VPI                        | N               |   |               |          |
| BGP Routing Proto                          | d               |   | ~             |          |
| Neeroestande de                            |                 |   |               |          |
| Enable automatic feat                      | ure key synchro | poization (Fireware OS v11.6.3 and higher)  |               |          |
|  | and hey aynome  |   | -             | _        |
| <ul> <li>Send alarm notificatio</li> </ul> | n when feature  | key is going to be expired or has been expired  | Notifications |          |
| (Fireware OS v11.10                        | 1 and higher)   |   |               | -10M     |
|  | and manely      |   |               |          |



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.

| terraces Link                | Aggregation                                  | Bridge            | VLAN L                              | .oopback                        | Bridg   | e Protocols     | WINS/DN | S Dynamic DI | NS Multi-WAN | PPPoE |
|------------------------------|--|-------------------|-------------------------------------|---------------------------------|---------|-----------------|---------|--------------|--------------|-------|
| DNS (Domain M                | lame System)                                 | Servers           |                                     |                                 |         |                 |         |              |              |       |
| Domain Name                  | con  | m                 |                                     |                                 |         |                 |         |              |              |       |
| DNS Servers                  | 8.8.8.8                                      |                   |                                     |                                 |         |                 | ~ ~     |              |              |       |
|                              |  |                   | 1.1000                              | Aug. (1997)                     |         | A DATE OF A DEC |         |              |              |       |
| Listen on a                  | NS Forwardin<br>I Trusted, Opt               | <b>g (Firew</b> a | are OS v1<br>I Custom i             | 1.12.2 and                      | t highe | r)<br>Select    |         |              |              |       |
| Listen on a<br>Conditional f | NS Forwardin<br>I Trusted, Opt               | <b>g (Firew</b> a | are OS v1<br>I Custom i             | 1.12.2 and                      | t highe | r)<br>Select    | ]       |              |              |       |
| Listen on a<br>Conditional f | NS Forwardin<br>I Trusted, Opt<br>forwarding | ig (Firewa        | are OS v1<br>I Custom i<br>DNS Serv | 1.12.2 and<br>nterfaces<br>vers | t highe | r)<br>Select    | _       |              |              |       |

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

|                   |   |                             |                         |                                    | N           | letwork (    | onfigu      | ration     |                |                |                          |
|-------------------|---|-----------------------------|-------------------------|------------------------------------|-------------|--------------|-------------|------------|----------------|----------------|--------------------------|
| Interfac          | ces Link Aggr   | egation                     | Bridge                  | VLAN Loo                           | pback Bri   | dge Protoco  | s WINS      | DNS D      | ynamic DNS     | Multi-WAN      | PPPoE                    |
| Multi-I<br>Selec  | WAN Configura<br>ct the method to                       | tion<br>route n             | on-IPSec                | traffic among                      | more than   | one extern   | al interfac | e. Click ( | Configure t    | o set more pr  | roperties.               |
| Rout              | ting Table  | -                           | Configure               |                                    |             |              |             |            |                |                |                          |
| Link M            | Ionitor Advan   | ced                         |                         |                                    |             |              |             |            |                |                |                          |
| Select<br>interfa | t a method for t<br>ace to check if<br>ternal Interface | he Fireb<br>the inter<br>s: | ox to use<br>face is ac | to check the<br>tive.<br>Settings: | status of e | sach externi | al interfac | e. By det  | ault, the Fire | ebox pings th  | e default gateway of the |
| EX                | T_MediaCom  |                             |                         | Monitor                            | EXT_Wind    | stream by:   | -           |            |                |                |                          |
| EX                | (T_Windstream   | 1                           |                         | Ping                               | IP Addres   | is V         |             |            |                |                |                          |
|                   |   |                             |                         | _ тср                              | IP Addres   | is v         | S           |            | Port:          | 80 😳           |                          |
|                   |   |                             |                         | Both                               | Ping and T  | 'CP must be  | successi    | ul to defi | ne the interi  | face as active | e                        |
|                   |   |                             |                         | Use thes                           | se settings | for EXT_W    | ndstrea     | n:         |                |                |                          |
|                   |   |                             |                         | Probe In                           | terval:     | 15 🔷         | Second      | s          |                |                |                          |
|                   |   |                             |                         | Deactive                           | ate After,  | 3 🗘          | Consec      | utive Fail | ures           |                |                          |
|                   |   |                             |                         | Reactive                           | ate After:  | 3 ~          | Reactive    | ate After  | E.             |                |                          |
|                   |   |                             |                         | Reactive                           | ste After:  | 3            | Reactiv     | ate After  | ÷              |                |                          |



|  |                   | Network Configuration                                  |                     |
|--|-------------------|--|---------------------|
| Interfaces Link Aggregation Bridg      | ge VLAN Loop      | back   Bridge Protocols   WINS/DNS   Dynamic DNS       | Multi-WAN PPPOE     |
| Multi-WAN Configuration                |                   |  |                     |
| Select the method to route non-IPS     | Sec traffic among | more than one external interface. Click Configure to s | et more properties. |
| Routing Table V Config                 | ure               |  |                     |
|  | I Ma              | Iti WAN Pouting Table Configuration                    | ×                   |
| Link Monitor Advanced                  |                   | In WAN Routing Table Configuration                     |                     |
| Coloris a method facility Simbou in    | Select inte       | erfaces for the Multi-WAN routing table configuration. | a the default       |
| interface to check if the interface is | s ac Include      | Interface  |                     |
| External Interfaces:                   |                   | EXT_MediaCom (0)                                       |                     |
| EXT_MediaCom                           |                   | EXT_Windstream (4)                                     |                     |
| EXT_Windstream                         |                   |  |                     |
|  |                   |  |                     |
|  |                   |  | office              |
|  |                   |  | CUYC                |
|  |                   |  |                     |

No VLANs.

| }       |                   |           |             |          | Network Co       | nfiguratio | n           |           |         |        |
|---------|-------------------|-----------|-------------|----------|------------------|------------|-------------|-----------|---------|--------|
| Interfi | aces Link Aggre   | gation Br | idge VLAN   | Loopback | Bridge Protocols | WINS/DNS   | Dynamic DNS | Multi-WAN | PPPoE   |        |
| Virtu   | al Local Area Net | work (VL4 | N) settings |          |                  |            |             |           |         |        |
| ID      | Name (Alias)      | Zone      | IPv4 Addre  | 165      | IPv6 Addre       | 55         | Seconda     | ry Inte   | erfaces | Add    |
|         |                   |           |             |          |                  |            |             |           |         | Edit   |
|         |                   |           |             |          |                  |            |             |           |         | Delete |
|         |                   |           |             |          |                  |            |             |           |         |        |
|         |                   |           |             |          |                  |            |             |           |         |        |
|         |                   |           |             |          |                  |            |             |           |         |        |

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.

|      |                    | Interface            | Settings - I   | nterface # 1 |        |
|------|--------------------|----------------------|----------------|--------------|--------|
| IPv4 | Pv6 Secondary      | MAC Access Contro    | Advanced       |              |        |
| Inte | rface Name (Alias) | Trusted              |                |              |        |
| Inte | rface Description: |                      |                |              |        |
| Inte | rface Type:        | Trusted              |                |              |        |
| IP A | Address:           | 130-000-0-00         |                |              |        |
| 0    | Disable DHCP       |                      |                |              |        |
|      | Lise DHCP Server   |                      |                |              |        |
|      | You can configur   | e a maximum of six a | idress ranges. |              |        |
|      | Address Pool       |                      |                |              |        |
|      | Starting IP        |                      | Ending IP      |              | Add    |
|      | -                  |                      | 192.168.3      | .150         | Edit   |
|      |                    |                      |                |              | Delete |
|      |                    |                      |                |              |        |
|      |                    |                      |                |              |        |
|      | Reserved Addres    | sses:                |                |              |        |
|      | Reserved Name      | Res                  | ervation IP    | MAC Address  | Add    |
|      |                    |                      |                |              | Edit   |
|      |                    |                      |                |              | Delete |
|      |                    |                      |                |              |        |
|      |                    |                      |                |              |        |
|      | Leasing Time 20    | ) days               |                |              | ~      |
|      |                    |                      |                |              | 100    |
|      | Configure DNS      | S/WINS servers       | DHCP Options   | 6 J          |        |



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

| Pv4  | IPv6 S  | Secondary  | MAC Access Co    | ntrol Advanced                                  |               |              |             |                         |   |                              |
|------|---|--|------------------|---|---------------|--------------|-------------|-------------------------|---|------------------------------|
| Inte | erface Na   | ame (Alias):                                     | Trusted          |   |               |              |             |                         |   |                              |
| Inte | erface De   | escription:                                      |                  |   |               |              |             |                         | _ |                              |
| Inte | erface Ty   | ype:   | Trusted          |   |               |              |             | ~                       |   |                              |
| IP A | Address:  |  | 102 102 2 102    |   |               |              |             | ~                       |   |                              |
| 0    | Dirable   | DHCD   |                  |   |               |              |             |                         | P | Fi                           |
|      | / Uisaulo   | i billor   |                  | 10  | C             | onfigure     | DNS/WIN     | S servers               |   |                              |
|      |   |  |                  |   |               |              |             |                         |   |                              |
| ۲    | Use DH  | ICP Server                                       | a maximum of si  |   |               |              |             |                         |   | _                            |
| ۲    | ) Use DH<br>You ca<br>Addre                             | ICP Server<br>an configure<br>tss Poot           | a maximum of st  | DNS Servers: (                                  | (If not defi  | ned, use the | Network DNS | Servers)                |   |                              |
| ۲    | Use DH<br>You ce<br>Addre<br>Startir                    | ICP Server<br>an configure<br>sss Poot<br>ing IP | a maximum of st  | DNS Servers: (<br>Domain Name:                  | ()f not defi  | ned, use the | Network DNS | Servers)                |   |                              |
| ۲    | Vou ca<br>Addre<br>Startir                              | ICP Server<br>an configure<br>ass Poot<br>ing IP | a maximum of si  | DNS Servers: (<br>Domain Name:                  | (If not defin | ned, use the | Network DNS | Servers)                |   | Add                          |
| ۲    | Vou ca<br>Addre<br>Startir                              | ICP Server<br>an configure<br>ess Poot<br>ing IP | a maximum of si  | DNS Servers: (<br>Domain Name:                  | (If not defin | ned, use the | Network DNS | Servers)                |   | Add<br>Edit                  |
| ۲    | Vou ca<br>Addre<br>Startir                              | ICP Server<br>an configure<br>ess Pool<br>ing IP | a maximum of sit | DNS Servers: (<br>Domain Name:                  | (If not defin | ned, use the | Network DNS | Servers)                |   | Add<br>Edit<br>Delete        |
| ۲    | Vise DH<br>You ca<br>Addre<br>Startin                   | ICP Server<br>an configure<br>ess Poot<br>ing IP | a maximum of sk  | DNS Servers: (<br>Domain Name:                  | (If not defin | ned, use the | Network DNS | Servers)<br>S Servers)  |   | Add<br>Edit<br>Delete        |
| ٠    | Vise DH<br>You ca<br>Addre<br>Startir<br>Reser<br>Reser | ICP Server<br>an configure<br>ess Poot<br>ing IP | a maximum of st  | DNS Servers: (<br>Domain Name:<br>WNIS Servers: | (If not defin | ned, use the | Network DNS | Servers)<br>IS Servers) |   | Add<br>Edit<br>Delete<br>Add |

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

|               |                                     | Sustam Managa        | Matchfuard                                  |                |                         |       |
|---------------|-------------------------------------|----------------------|---|----------------|-------------------------|-------|
|               | ×                                   | rface # 1            | face Settings - Inte                        | Inte           |                         |       |
|               |                                     |                      | Control Advanced                            | MAC Access     | Secondary               | IPv4  |
|               |                                     |                      |   | Trusted        | Name (Alias):           | Inter |
|               |                                     |                      |   |                | Description:            | Inter |
|               | ~                                   |                      |   | Trusted        | Гуре:                   | Inter |
| <b>—</b>      | ~ ×                                 |                      |   |                | s:                      | PAd   |
|               |                                     |                      |   |                | le DHCP                 | 01    |
| Tags          |                                     |                      |   |                | HCP Server              | ۱     |
|               |                                     |                      | six address ranges.                         | a maximum of   | can configure           | _     |
|               |                                     | ICP Options          | DI  |                |                         | 1     |
|               |                                     |                      |   |                |                         |       |
|               | dd your own Custom option.          | defined options or a | <sup>o</sup> Server. Choose from Pr         | ns for the DHC | d DHCP Option           |       |
| Add.          | dd your own Custom option.<br>Value | defined options or a | <sup>o</sup> Server. Choose from Pr         | ns for the DHC | d DHCP Option<br>e Name |       |
| Add.<br>Edit. | dd your own Custom option.<br>Value | defined options or a | <sup>9</sup> Server. Choose from Pr<br>Type | ns for the DHC | d DHCP Option<br>e Name |       |

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

| IPv4 | IPv6 Secondary                    | MAC Access     | Control Advanced    |             |   |
|------|-----------------------------------|----------------|---------------------|-------------|---|
| Inte | rface Name (Alias):               | VOIP-IP-4      |                     |             |   |
| Inte | rface Description:                | VOIP-4.0       |                     |             |   |
| Inte | rface Type:                       | Optional       |                     |             | 0                                       |
| IP A | ddress:                           |                |                     |             | 1                                       |
| •    | Disable DHCP<br>Use DHCP Server   |                |                     |             |   |
|      | You can configure                 | e a maximum of | six address ranges. |             |   |
|      | Address Poor                      |                | Endino F            | 3           | Add                                     |
|      |                                   |                |                     |             |   |
|      |                                   |                | 1.000               |             | Edd                                     |
|      |                                   |                |                     |             | Edit<br>Delete                          |
|      | Reserved Addres                   | 505:           | 1                   |             | Edit                                    |
|      | Reserved Addres<br>Reserved Name  | 505:           | Reservation IP      | MAC Address | Edit<br>Delete                          |
|      | Reserved Addres<br>Reserved Name  | 505:           | Reservation IP      | MAC Address | Edit<br>Delete<br>Add<br>Edit           |
|      | Reserved Addres<br>Reserved Name  | SCS:           | Reservation IP      | MAC Address | Edit<br>Delete<br>Add<br>Edit<br>Delete |
|      | Reserved Addres<br>Reserved Name  | SCS:           | Reservation IP      | MAC Address | Add Edit Delete                         |
|      | Reserved Address<br>Reserved Name | scs:           | Reservation IP      | MAC Address | Add Edit                                |

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



| Use NTP to syn | chronize the system | n time |  |
|----------------|---------------------|--------|--|
| 0.pool.ntp.org | esne Audresses:     |        |  |
| 1.pool.ntp.org |                     |        |  |
| - providence a |                     |        |  |
|                |                     |        |  |
|                |                     |        |  |
|                |                     |        |  |
|                |                     | A      |  |

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.

| Edit Doline Departies  | Edit Policy Properties   |        |
|--|--|--------|
| Name: WatchGuard Web UI  | Name: WatchGuard   | 🗹 Enai |
|  | Policy Properties Advanced   |        |
| Policy Properties Advanced   | WG-Firebox-Mgmt connections are  |        |
| WG-Fireware-XTM-WebUI connections are  | Allowed v Send TCP RST   |        |
| Allowed V Send TOP RST   | From   |        |
| From   | Any-Trusted  |        |
| Any-Trusted  | Any-Optional   |        |
| Any-Optional   | A Restaure (Finalese DB)   |        |
| 24   | inantus (reebox-ub)  |        |
| Parameter and a second se | - Add Edit Ray   | move   |
| Add Edit Remove  | To   |        |
| To   | Firebox  | 1      |
| 1 Firebox  |  |        |
|  | 2  |        |
|  |  |        |
|  | Add. Edt. Re   | move   |
| Add Edt Remove   | Route outbound traffic using SD-WAN Based Routing (Freware OS v12.3 or higher) |        |
| Route outbound traffic using SD-WAN Based Routing (Fireware OS v12.3 or higher)  |  |        |
| SD-WAN Action  | SU-WAN ACDON   |        |
|  |  |        |
|  |  |        |
| Enable Application Control: Global 🛛 🕅   |  |        |



| 10       |              |                               | C:\Users\Admini         | istrator.                    |   | -M200_11_10_2.xml         | *- Fireware Polic | / Manager   |        |    |
|----------|--------------|-------------------------------|-------------------------|------------------------------|---|---------------------------|-------------------|-------------|--------|----|
| File Edi | t View Setu  | p Network FireCluster VPN Sub | scription Services Help |                              |   |                           |                   |             |        |    |
| -        |              | + X 🗄 🖉 🐘 🗎 🖓 🐇               |                         |                              |   |                           |                   |             |        |    |
|          |              |                               | 1                       |                              |   |                           |                   |             |        |    |
| Firewai  | Mobile VPN w | th IPSec                      |                         |                              |   |                           |                   |             |        |    |
|          |              |                               |                         |                              |   |                           |                   |             |        | Fi |
| Order /  | Action       | Policy Name                   | Policy Type             | From                         | To  | Port                      | PBR SD-WAN        | App Control | Tags V | 7. |
| 1        | 1            | LDAP to DCs.gs.parts          | LDAP                    | Any-Trusted                  | GroupDC   | tcp:389                   |                   | None        |        |    |
| 2        | 1            | Ping. 1                       | Ping                    | Any-Trusted                  | Any-External, Any-BOVPN   | icmp (type: 8, code: 255) |                   | None        |        |    |
| 3        | 1            | DNS to EH                     | DNS                     | Any-Trusted                  | 1   | tcp:53 udp:53             |                   | None        |        |    |
| 4        | 1            | Global                        | Global Cli.             | . Any-Trusted                | 1   | tcp:22490 tcp:1433 udp:1  |                   | None        |        |    |
| 5        |              | SMB to                        | SMB                     | Any-Trusted                  |   | tcp:445 udp:445 udp:137   |                   | None        |        |    |
| 6        | 1            | Any DFS Replia DU -EH         | Any                     | 192.16                       |   | any                       |                   | None        |        |    |
| 7        | 1            | ANY to DC EH                  | Any                     | 192.100.0.101, 102.100.0.1   | GroupDC   | any                       |                   | None        |        |    |
| 8        | 1            | Firewall Bypass               | Any                     | NWADMIN ( n)                 | Any-External  | any                       |                   | None        |        |    |
| 9        | 1            | E FTP                         | FTP                     | Any-Trusted, Any-Optional    | Any-External  | tcp:21                    |                   | None        |        |    |
| 10       | 0            | Wirless_to_Wired              | Wirlass_to_Wired        | Trusted, Any-BOVPN           |   |                           |                   | None        |        |    |
| 11       | $\checkmark$ | WatchGuard Authentication     | WG-Auth                 | Any-Trusted, Any-Optional, . | Firebox   | tcp:4100                  |                   | None        |        |    |
| 12       | 1            | WatchGuard Web UI             | WG-Fireware-XTM         | Any-Trusted, Any-Optional, . | Firebox   | tcp:8080                  |                   | None        |        |    |
| 13       | 1            | (3) Ping                      | Ping                    | Any-Trusted, Any-Optional    | Any   | icmp (type: 8, code: 255) |                   | None        |        |    |
| 14       | 1            | WatchGuard                    | WG-Firebox-Mgmt         | Any-Trusted, Any-Optional, . | Firebox   | tcp:4105 tcp:4117 tcp:41  |                   | None        |        |    |
| 15       | 1            | Navision                      | Navision                | Any-Trusted, Any-External    | P   | tcp:2000-3000             |                   | None        |        |    |
| 16       | 1            | TU to RDS Gateway             | HTTPS                   | Any-Trusted                  |   | tcp:443                   |                   | None        |        |    |
| 17       | 1            | DFS Replica DU-EH             | DFS Replica             | 192.168.3.183                |   | tcp:135 tcp:445 tcp:4915  |                   | None        |        |    |
| 18       | 1            | Cutgoing                      | TCP-UDP                 | Any-Trusted, Any-Optional    | Any-External  | tcp:0 (Any) udp:0 (Any)   |                   | None        |        |    |
| 19       | 0            | EFTP-proxy                    | FTP-proxy               | Any-Trusted                  | Any-External  | tcp:21                    |                   | None        |        |    |
| 20       |              | POP3-proxy                    | POP3-proxy              | Any-Trusted                  | Any-External  | tcp.110                   |                   | None        |        |    |
| 21       | 0            | W HTTP-proxy                  | HTTP-proxy              | Any-Trusted                  | Any-External  | tcp:80                    |                   | None        |        |    |
| 22       | 0            | DNS-proxy                     | DNS-proxy               | Any-Trusted                  | Any-External  | tcp:53 udp:53             |                   | None        |        |    |
| 23       | 1            | 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       | 1            | WatchGuard SSLVPN             | SSL-VPN                 | Any-External, Any-Trusted, . | Firebox   | tcp:443                   |                   | None        |        |    |
| 26       | X            | Any Deny to I                 | Any                     | Any-Trusted                  | the second s  | any                       |                   | None        |        |    |
| 27       | 1            | Allow SSLVPN-Users            | Any                     | SSLVPN-Users (Any)           | Any   | any                       |                   | None        |        |    |
| 28       | 0            | SQL to EH                     | SOL to EH               |                              |   | tcp:1433 tcp:1434         |                   | None        |        |    |
| 29       | 1            | BOVPN-Allow.in                | Any                     |                              | Any   | any                       |                   | None        |        |    |
| 30       | 1            | BOVPN-Allow.out               | Any                     | Any                          | The second se | 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.



| llow Mobile VP  | N with SSL connections from the internet to the external interface.   |
|---|---|
| Activate Mo   | bile VPN with SSL   |
| General Auth  | entication Advanced   |
|   |   |
| Type or sel   | locresses<br>lect a Firebox IP address or domain name for SSL VPN users to connect to.  |
| Primary:  | Backup: and an an   |
| , mary.   |   |
| Networking  | and IF Address Fool   |
|   |   |
| Choose the  | e method the Firebox uses to send traffic through the VPN tunnel. Select Bridge VPN traffic if you want<br>a user to a network you enacity. Select Poute VPN traffic if you want the Firebox to route VPN traffic   |
| Choose the<br>to bridge th<br>to specified  | Emethod the Firebox uses to send traffic through the VPN tunnel. Select Bridge VPN traffic if you want<br>is user to a network you specify. Select Route VPN traffic if you want the Firebox to route VPN traffic<br>i networks and resources.  |
| Choose the<br>to bridge th<br>to specified  | Emethod the Firebox uses to send traffic through the VPN tunnel. Select Bridge VPN traffic if you want<br>le user to a network you specify. Select Route VPN traffic if you want the Firebox to route VPN traffic<br>in networks and resources.   |
| Choose the<br>to bridge th<br>to specified<br>Routed VF   | e method the Firebox uses to send traffic through the VPN tunnel. Select Bridge VPN traffic if you want<br>te user to a network you specify. Select Route VPN traffic if you want the Firebox to route VPN traffic<br>d networks and resources.   |
| Choose the<br>to bridge th<br>to specified<br>Routed VF   | e method the Firebox uses to send traffic through the VPN tunnel. Select Bridge VPN traffic if you want<br>te user to a network you specify. Select Route VPN traffic if you want the Firebox to route VPN traffic<br>d networks and resources.<br>PN traffic   |
| Choose the<br>to bridge th<br>to specified<br>Routed VF   | e method the Firebox uses to send traffic through the VPN tunnel. Select Bridge VPN traffic if you want<br>te user to a network you specify. Select Route VPN traffic if you want the Firebox to route VPN traffic<br>d networks and resources.<br>PN traffic   |
| Choose the<br>to bridge th<br>to specified<br>Routed VF   | e method the Firebox uses to send traffic through the VPN tunnel. Select Bridge VPN traffic if you want<br>the user to a network you specify. Select Route VPN traffic if you want the Firebox to route VPN traffic<br>d networks and resources.<br>PN traffic  |
| Choose the<br>to bridge th<br>to specified<br>Routed VF   | e method the Firebox uses to send traffic through the VPN tunnel. Select Bridge VPN traffic if you want<br>the user to a network you specify. Select Route VPN traffic if you want the Firebox to route VPN traffic<br>d networks and resources.<br>PN traffic  |
| Choose the<br>to bridge th<br>to specified<br>Routed VF   | e method the Firebox uses to send traffic through the VPN tunnel. Select Bridge VPN traffic if you want<br>the user to a network you specify. Select Route VPN traffic if you want the Firebox to route VPN traffic<br>d networks and resources.<br>PN traffic  |
| Choose the<br>to bridge th<br>to specified<br>Routed VF<br>Force :<br>Allo<br>Spe<br>19                         | emethod the Firebox uses to send traffic through the VPN tunnel. Select Bridge VPN traffic if you want<br>the user to a network you specify. Select Route VPN traffic if you want the Firebox to route VPN traffic<br>d networks and resources.<br>2N traffic v<br>all client traffic through tunnel<br>w access to all Trusted, Optional, and Custom networks<br>scify allowed resources<br>2  |
| Choose the<br>to bridge th<br>to specified<br>Routed VF<br>Force :<br>Allo<br>Spe<br>19                         | e method the Firebox uses to send traffic through the VPN tunnel. Select Bridge VPN traffic if you want<br>the user to a network you specify. Select Route VPN traffic if you want the Firebox to route VPN traffic<br>d networks and resources.<br>PN traffic v<br>all client traffic through tunnel<br>w access to all Trusted, Optional, and Custom networks<br>selfy allowed resources<br>12  |
| Choose the<br>to bridge th<br>to specified<br>Routed VF<br>Force of<br>Allo<br>Specified                        | a method the Firebox uses to send traffic through the VPN tunnel. Select Bridge VPN traffic if you want<br>the user to a network you specify. Select Route VPN traffic if you want the Firebox to route VPN traffic<br>d networks and resources.  N traffic  N traffic  N all client traffic through tunnel  w access to all Trusted, Optional, and Custom networks selfy allowed resources  Add  Remove  |
| Choose the<br>to bridge th<br>to specified<br>Routed VF<br>Force 0<br>Allo<br>© Spe<br>19                       | Internoot the Firebox uses to send traffic through the VPN tunnel. Select Bridge VPN traffic if you want<br>the user to a network you specify. Select Route VPN traffic if you want the Firebox to route VPN traffic<br>d networks and resources.<br>It for the user to a network the firebox to route VPN traffic<br>all client traffic through tunnel<br>w access to all Trusted, Optional, and Custom networks<br>selfy allowed resources<br>Iz<br>PAdd Remove<br>IP Address Pool  |
| Choose the<br>to bridge th<br>to specified<br>Routed VF<br>Force :<br>Allo<br>Specified<br>Virtual<br>Specified | a method the Firebox uses to send traffic through the VPN tunnel. Select Bridge VPN traffic if you want<br>to user to a network you specify. Select Route VPN traffic if you want the Firebox to route VPN traffic<br>d networks and resources.<br>N traffic v<br>all client traffic through tunnel<br>w access to all Trusted, Optional, and Custom networks<br>scify allowed resources<br>12<br>Add Remove<br>P Address Pool<br>y the private IP addresses to assign to Mobile VPN with SSL users. Your Firebox allows 75 Mobile                              |
| Choose the<br>to bridge th<br>to specified<br>Routed VF<br>Force :<br>Allo<br>• Spe<br>19                       | a method the Firebox uses to send traffic through the VPN tunnel. Select Bridge VPN traffic if you want<br>the user to a network you specify. Select Route VPN traffic if you want the Firebox to route VPN traffic<br>d networks and resources.<br>N traffic v<br>all client traffic through tunnel<br>w access to all Trusted, Optional, and Custom networks<br>scify allowed resources<br>12<br>• • • / Add Remove<br>IP Address Pool<br>y the private IP addresses to assign to Mobile VPN with SSL users. Your Firebox allows 75 Mobile<br>vith SSL users. |

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.

| ow Mobile \   | /PN with SSL connections fro  | in the internet to the ex   | dernal interface.   | PN' policy are crea  |
|---|---|---|---|----------------------|
| Activate N  | Jobile VPN with SSL   |   |   |                      |
| eneral Au   | uthentication Advanced  |   |   |                      |
| Authentica  | tion Server Settings  |   |   |                      |
| Select on   | e or more authentication serve  | ers. The first server in  | the list is the default authenticat   | ion                  |
| server, To  | configure additional authenti   | cation servers, click C   | onfigure.   |                      |
| Select  | Authentication Server   |   | Config  | ure                  |
|   | Eirabox DB  |   | Make D  | efault               |
|   |   |   |   |                      |
| Auto  | reconnect after a connection  | is lost   |   |                      |
| Auto  | reconnect after a connection<br>rce users to authenticate after<br>the Mobile VPN with SSL clie   | is lost<br>er a connection is lost<br>ent to remember passw   | rord  |                      |
| Auto  | reconnect after a connection<br>orce users to authenticate after<br>the Mobile VPN with SSL clie<br>ware OS v11.8 and higher)   | is lost<br>er a connection is lost<br>ent to remember passw   | rord  |                      |
| Auto<br>Auto<br>Fo<br>Allow<br>(Fire<br>Users and<br>Specify th<br>to the SSI | reconnect after a connection<br>roe users to authenticate after<br>the Mobile VPN with SSL clie<br>ware OS v11.8 and higher)<br>Groups<br>te users and groups for Mobil<br>VPN-Users group.   | is lost<br>ar a connection is lost<br>int to remember passw<br>le VPN with SSL. The u   | ord   | re automatically adv |
| Auto Auto Fo Allow (Fire Users and Specify th to the SSI                      | reconnect after a connection<br>roe users to authenticate after<br>the Mobile VPN with SSL clie<br>ware OS v11.8 and higher)<br>Groups<br>te users and groups for Mobil<br>VVPN-Users group.<br>Name  | is lost<br>ar a connection is lost<br>int to remember passw<br>le VPN with SSL. The u<br>Type   | ord<br>sers and groups you specify a<br>Authentication Server   | re automatically add |
| Auto Fo Fo Allow (Fire Users and Specify tt to the SSI                        | reconnect after a connection<br>troe users to authenticate after<br>the Mobile VPN with SSL cie<br>ware OS v11.8 and higher)<br>Groups<br>te users and groups for Mobil<br>VPN-Users group.<br>Name<br>SSLVPN-Users                                   | is lost<br>er a connection is lost<br>ent to remember passw<br>le VPN with SSL. The u<br>Type<br>Group                                  | ord sers and groups you specify a Authentication Server Any   | re automatically add |
| Auto     Fo     Fo     Specify th     to the SSI     O                        | reconnect after a connection<br>rore users to authenticate afte<br>the Mobile VPN with SSL clie<br>ware OS v11.8 and higher)<br>Groups<br>te users and groups for Mobil<br>V2PH-Users group.<br>Name<br>SSL/VPH-Users<br>Markus                       | is loat<br>er a connection is lost<br>int to remember passw<br>le VPN with SSL. The u<br>Type<br>Group<br>User                          | ord sers and groups you specify a Authentication Server Any Firebox-DB  | re automatically add |
| Auto     Fo     Fo     Vers and     Specify th     to the SSI     Vers        | reconnect after a connection<br>rce users to authenticate after<br>the Mobile VPN with SSL clic<br>ware OS v11.8 and higher)<br>Groups<br>te users and groups for Mobil<br>_VPN-Users group.<br>Name<br>SSLVPN-Users<br>Markus<br>NVXADINN            | is lost<br>er a connection is lost<br>int to remember passw<br>le VPN with SSL. The u<br>Type<br>Group<br>User<br>User<br>User          | ord sers and groups you specify a Authentication Server Any Firebox-DB Firebox-DB                                   | re automatica®y ada  |
| Auto Fo Fo Auto (Fire Users and Specify th to the SSI                         | reconnect after a connection<br>rore users to authenticate after<br>the Mobile VPN with SSL clie<br>ware OS v11.8 and higher)<br>Groups<br>e users and groups for Mobil<br>VPH-Users group.<br>Name<br>SSLVPH-Users<br>Markus<br>NVA-DUNN<br>NVA-DUNN | is lost<br>rr a connection is lost<br>int to remember pass w<br>le VPN with SSL. The L<br>Type<br>Group<br>User<br>User<br>User<br>User | ord Isers and groups you specify a Authentication Server Any Firebox-DB Firebox-DB Firebox-DB Firebox-DB Firebox-DB | re automatically ad  |

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.



| low Mobile VPN with                                     | SSL conne                                    | ctions                       | from th | e Inter                     | net t                     | to the          | ext  | erna         | al interface.  | LIC. |
|---|--|------------------------------|---------|-----------------------------|---------------------------|-----------------|------|--------------|--|------|
| Activate Mobile VI                                      | N with SSL                                   | 1                            |         |                             |                           |                 |      |              |  |      |
| General Authentica                                      | tion Adva                                    | nced                         |         |                             |                           |                 |      |              |  |      |
| Authentication:   | S  | HA-1                         |         |                             | _                         |                 |      | ~            |  |      |
| Encryption:   | A  | ES (256                      | 5-bit)  |                             |                           |                 |      | ¥            |  |      |
| Data channel:   | т  | CP                           | ~       |                             |                           | 4               | 43   | •            |  |      |
| Configuration chan                                      | net: TC                                      | Ρ                            |         |                             |                           | 4               | 43   | ^<br>V       |  |      |
| Keep-alive:   | Int  | erval:                       |         | 10                          | ~ >                       | seci            | ond  | 5            |  |      |
|   | Tir  | neout                        |         | 60                          | ~ >                       | seci            | ond  | 8            |  |      |
| Renegotiate data ch                                     | annel: Int                                   | erval:                       |         | 480                         | ^<br>¥                    | minu            | ites |              |  |      |
| DNS and WINS Se   | invers                                       |                              |         |                             |                           |                 |      |              |  |      |
| For Mobile VPN v<br>domain name and<br>Configuration do | vith SSL clie<br>at least on<br>not apply to | ents to r<br>e DNS<br>Mobile | or WINS | unqua<br>S servi<br>vith SS | alifie<br>er. T<br>iL cli | d nam<br>he Fil | rebo | and<br>ix Di | FQDNs for your domain, you must specif<br>NS settings you specified in the Network | y a  |
| Domain name:  |  | m                            |         |                             |                           |                 |      |              |  |      |
|   |  |                              | 45      |                             |                           | 8 .             | 8    | . 8          | 8  |      |

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.

|  | Single Sign-On Term  | inal S   | Services Authentication Portal  |
|--|--|--|---|
| rewall Authenticatio   | n  |  |   |
| imeout settings appl<br>to not already have a  | y to users who authent<br>a timeout configured. If   | icate<br>you s                                   | to external, third-party authentication servers that<br>select a value of zero, a timeout does not occur.   |
| Session Timeout  | 0  | +  | seconds ~   |
| Idle Timeout:  | 2  | ÷  | hours ~   |
| ogin limits apply to a<br>hat limit takes preced   | I users. If you specify<br>lence over this global s  | a diff<br>etting                                 | ferent login limit in the user or group settings,<br>g.   |
| Allow unlimited c  | oncurrent firewall auth  | entica   | ation logins from the same account  |
| C Limit concurrent   | user sessions to   |  | 1 0   |
| When the limit is r  | reached. Reject subse  | que  | nt login attempts   |
|  |  |  |   |
| The host name<br>that this host n<br>the host name<br>Send a redirect t  | must match the Comm<br>ame is specified in the<br>is the IP address of the<br>o the browser after sur  | on Na<br>DNS<br>devi                             | ame (CN) from the web server certificate. Make su<br>settings for your organization, and that the value o<br>ice.   |
| The host name<br>that this host n<br>the host name<br>Send a redirect to<br>Type the URL to<br>automatically gor   | must match the Comm<br>ame is specified in the<br>is the IP address of the<br>o the browser after sur<br>use for the redirect. Af<br>is to this URL (For exa                   | on Na<br>DNS<br>devi<br>ccess<br>ter si<br>mple, | ame (21) from the web server certificate. Make su<br>settings for your organization, and that the value o<br>lose.<br>Sful authentication<br>uccessful authentication, the user's browser,<br>http://company.com)   |
| The host name that this host in the host name the host name Send a redirect to automatically goe Management Sess   | must match the Comm<br>ame is specified in the<br>is the IP address of the<br>o the browser after sur<br>use for the redirect. Af<br>is to this URL. (For exa                  | on Na<br>DNS<br>devi<br>coesi<br>ter si<br>mple, | ame (2N) from the web server certificate. Make su<br>settings for your organization, and that the value o<br>loss.<br>All authentication<br>uccessful authentication, the user's browser<br>, http://company.com)   |
| The host name<br>that this host r<br>that this host r<br>that this host rame<br>Send a redirect to<br>Type the URL to<br>automatically gor<br>Annagement Sess<br>Session Timeout:  | must match the Comm<br>mane is specified in the<br>is the IP address of the<br>o the browser after sur<br>use for the redirect. Af<br>is to this URL (For exa<br>ion           | on Na<br>DNS<br>i devi<br>ccess<br>res<br>mple,  | ame (20) from the web server certificate. Make su<br>settings for your organization, and that the value o<br>ice. Set authentication<br>uccessful authentication, the user's browser<br>. http://company.com)       |
| The host name that this host n the host name that this host n the host name set of thost name set of the host name set of the host name | must match the Comm<br>ame is apecified in the<br>is the P address of the<br>o the browser after su-<br>use for the redirect. Af<br>as to this URL (For exa<br>ion<br>10<br>15 | on Na<br>DNS<br>devi<br>coesi<br>ter si<br>mple, | ame (CII) from the web server certificate. Make su<br>settings for your organization, and that the value of<br>ice.<br>shall authentication<br>cocessful authentication, the user's browser<br>.http://company.com) |

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.



| E Edit Active Directory Domai                        | n                                  | >                |
|--|------------------------------------|------------------|
|  |                                    |                  |
| Make sure that your users ca<br>servers you specify. | n successfully authenticate to the | Active Directory |
| Domain Name:   | SCHNA.com                          |                  |
| IP Address / DNS Name:                               | IP / DNS Port                      | Add              |
|  | 192.168.3.45 389                   | Remove           |
| Timeout  | 10                                 | seconds          |
| Dead Time  | 10 🗘                               | minutes ~        |
| Search Base:   | C-COM                              |                  |
| Group String   | tokenGroups                        |                  |
| Login Attribute:                                     | sAMAccountName ~                   |                  |
| DN of Searching User:                                | +Users,DC+                         |                  |
|  |                                    |                  |

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.