Client A

Report Prepared on 5th June 2023

Assessor: Felicia King, CISO and network security architect

Table of Contents

Relevant QPC Links 1

Discovery meeting data and findings 1

4Hr Premium RMA 5

Hardware 6

Services 6

Rearchitect network 6

Alternative configuration move and WAP only 6

Optional proactive management services 7

Pricing for recommended products 7

About 7

Relevant QPC Links

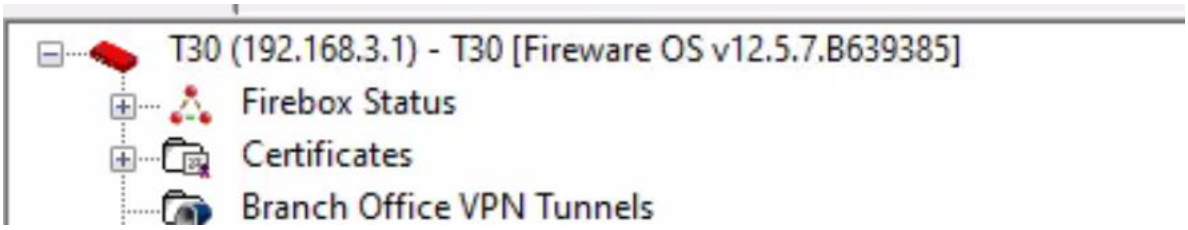
- https://www.qpcsecurity.com/category/in-the-news/
- https://www.qpcsecurity.com/2023/04/14/qpc-security-at-the-watchguard-partner-conference/

Discovery meeting data and findings

Site info: One site, Spectrum is ISP
Firebox serves as primary perimeter device
https://192.168.3.1:8080

- POS – system not on an isolated VLAN
- Office computers are expected to be secured.
- Current WAPs are provided PoE injectors.

Observed that the Fireware is quite old and a service plan should be in place to keep the Firebox Fireware versions maintained and configuration updated.



Note interface configuration and there is only a single VLAN which is Optional security zone. This means that the wireless is not setup properly in a segmented/isolated way, which is the intent of guest wireless at the club. Recommend QPC to rearchitect the network as part of the implementation of WAPs that are compatible with a new model Firebox. The network rearchitecture is also recommended because the easiest way to have PCI compliance is full isolation of the point of sale system.

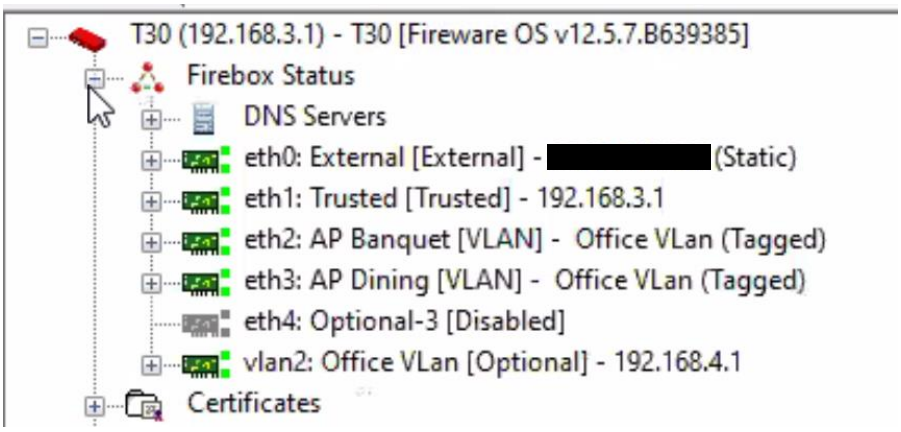
QPC has >20 years of experience supporting retail environments with point of sale. We would implement an isolated VLAN which can access the POS resources but is separated from guest and separated from office computers which could laterally compromise the point of sale system. PCI compliance requires network isolation and segmentation. It is also easy for us to accomplish this. The POS system would need to be direct wired back to an interface on the Firebox rather than going to through another switch. It is likely that the existing network cabling connectivity options already support this. In discussion with client's technical contact, it was determined that the switch at the business does not support VLANs with link aggregation, therefore we would want the WAPs and POS system directly attached to the Firebox. There are enough interfaces to accomplish this on both recommended Fireboxes.

The T30 Firebox is past end of life. This is the end-of-life policy page https://www.watchguard.com/wgrd-trust-center/end-of-life-policy.

QPC recommends replacement hardware which is either the T45-PoE or a T85-PoE. Note that the business currently uses two AP300 which are also end of life and not migratable to be compatible with any new Fireboxes. The T45-PoE has a single PoE port. The T85 has two PoE ports. In the case of two APs, QPC would normally deploy a T85 in order to avoid use of an external PoE injector. It simplifies and lowers the cost of supporting the wireless.

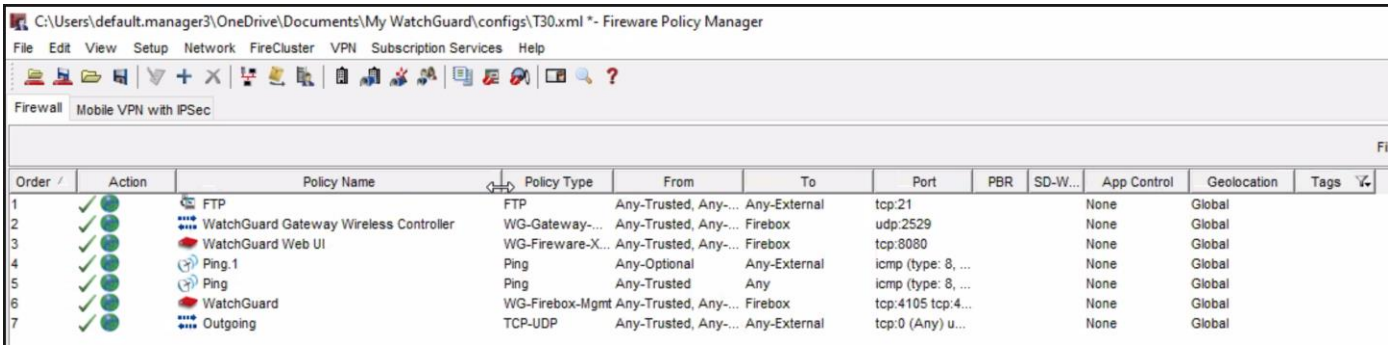
The existing PoE injectors for the older model WatchGuard APs may work for the new APs, but we have not tested that and cannot guarantee it. In discussion with client's technical contact, he confirmed that the current rack has a UPS and that PoE injectors are plugged into the UPS in battery protected outlets, not just surge protected outlets. APs must be in battery protected outlets when combined with PoE injectors.

From a horsepower perspective, the T45-PoE would have adequate horsepower in a scenario where the desire is to provide security protection to POS network and office network, while providing only very light security protection for guest. Generally businesses do not want to allow guests to access content which is outright malicious, criminal, or in violation with their business operations. Therefore items that would normally be blocked on guest would be pornography, viruses, malware, and criminal hosting sites. Otherwise guest access can be setup fairly unrestricted. A business that provides guest wireless with no web content filtering puts itself at risk of having its ISP connection shut off by the FBI if it is found that there is malicious traffic coming from the business IP address space.



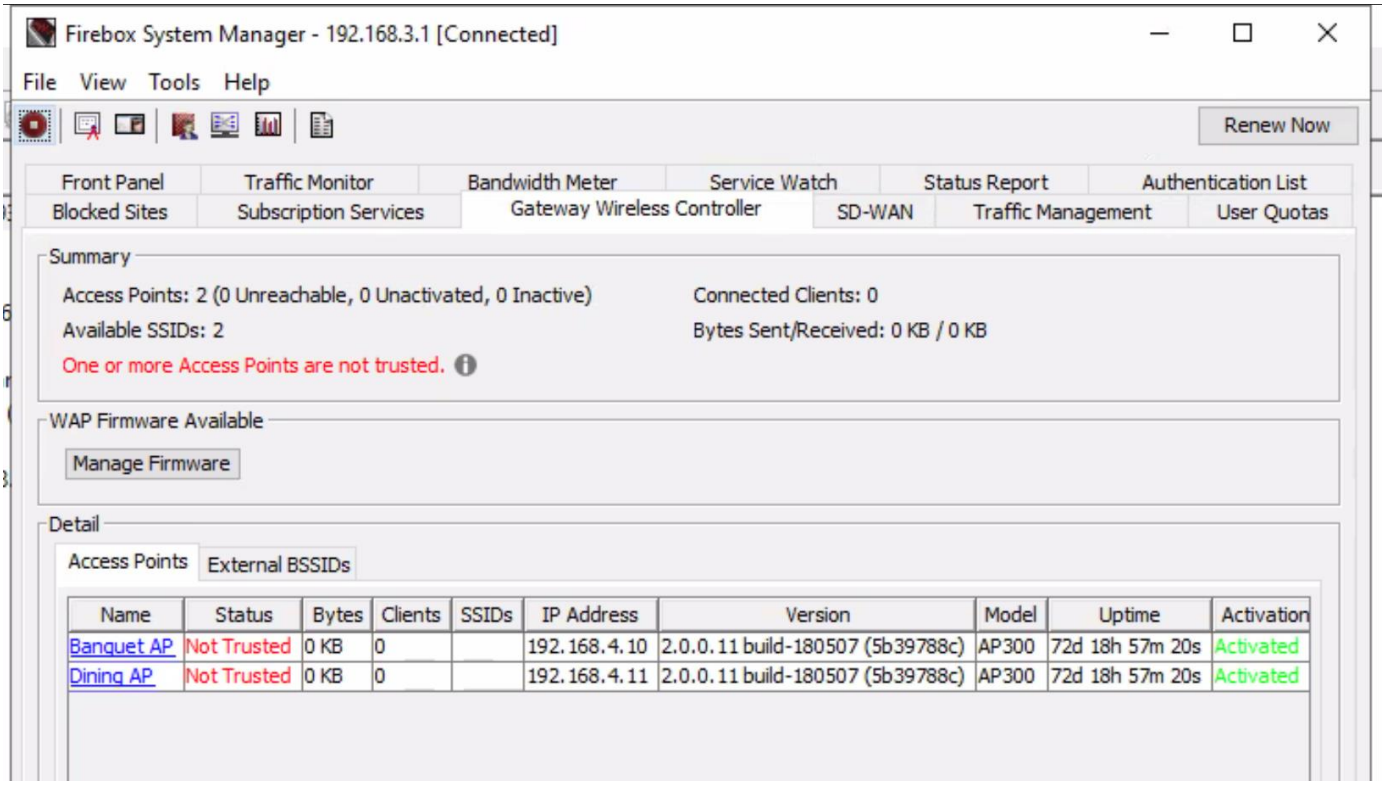
Please note that this configuration for VLAN 2 which is used for the WAPs does not actually provide segmentation and isolation. The way it is currently setup allows guests to attempt to hack the WAPs themselves and guests to hack other guests. Properly setup wireless avoids all of those problems and also would provide an office (trusted) wireless and a guest (untrusted) wireless.

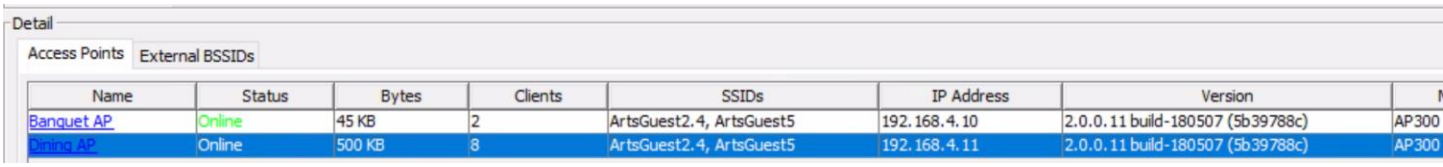
It is also prudent to mention that the below current policy configuration in the Firebox does not leverage the benefits of the security suite. It provides ingress protection from hackers making inbound connections, but there is no egress or outbound filtering / protection configured. Therefore, in order to leverage the value of the security suite, the Firebox would need to be properly programmed.



Order	Action	Policy Name	Policy Type	From	To	Port	PBR	SD-W...	App Control	Geolocation	Tags
1	✓	FTP	FTP	Any-Trusted, Any-...	Any-External	tcp:21			None	Global	
2	✓	WatchGuard Gateway Wireless Controller	WG-Gateway-...	Any-Trusted, Any-...	Firebox	udp:2529			None	Global	
3	✓	WatchGuard Web UI	WG-Fireware-X...	Any-Trusted, Any-...	Firebox	tcp:8080			None	Global	
4	✓	Ping.1	Ping	Any-Optional	Any-External	icmp (type: 8, ...			None	Global	
5	✓	Ping	Ping	Any-Trusted	Any	icmp (type: 8, ...			None	Global	
6	✓	WatchGuard	WG-Firebox-Mgmt	Any-Trusted, Any-...	Firebox	tcp:4105 tcp:4...			None	Global	
7	✓	Outgoing	TCP-UDP	Any-Trusted, Any-...	Any-External	tcp:0 (Any) u...			None	Global	

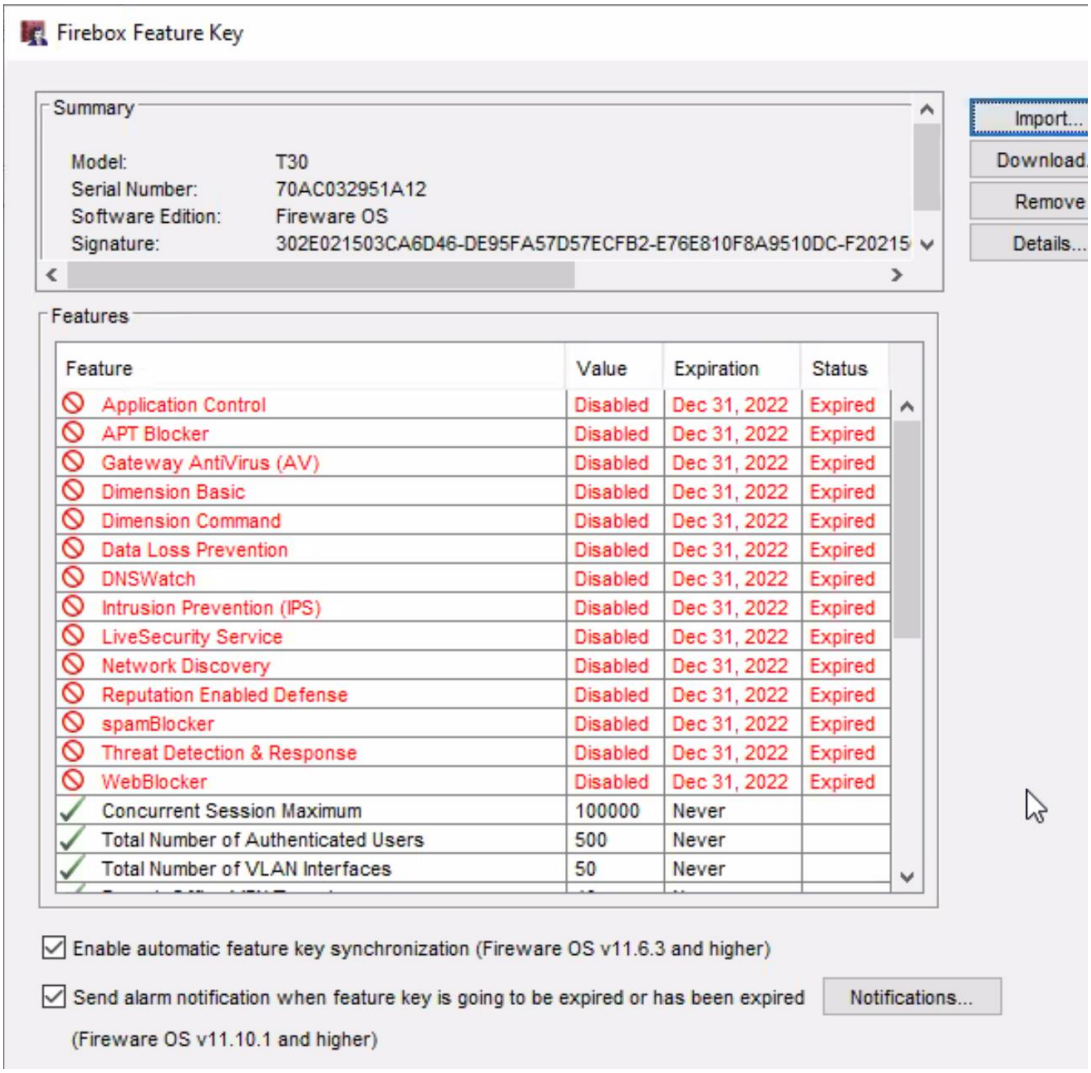
Two current APs are also past end of life and cannot be incorporated into a new Firebox.
During our meeting, I assisted Dave to get the APs listed as Trusted.
If there is more than one SSID now, it should be noted that all wireless traffic backhauls on the same VLAN and the same security zone. POS traffic and secure business traffic should not be on the same wireless as the guest traffic.





The current subscription is expired and has been expired for some time.

The former subscription was TSS (Total Security Suite). TSS is the correct subscription to get, but it must be paired with a proper configuration in order to leverage the benefits of the subscription.



4Hr Premium RMA

We encourage all business leaders to think about the amount of outage downtime that is tolerable. The hardware warranty support contract with TSS includes next business day warranty. If a business experiences an outage on a Friday, it could be until the following Wednesday that they are back up and running.

Example:

Hardware failure occurs on Friday. Tech support is contacted and issues RMA. Depending on the time of day, it may not ship out until Monday. If Monday is a Federal holiday, then the replacement hardware will not be received until late on Tuesday. Then tech support needs to be contacted in order to get configuration put into the replacement Firebox. Therefore, it is not likely until Wednesday when the business will be back fully functional.

Because of this, we strongly recommend the 4Hr Premium RMA service. It is exactly what it sounds like. They get you replacement hardware within 4 hours of a confirmed and authorized

RMA. It is offered in physical locations where they can deliver equipment. Madison, WI is a covered location, but some remote locations in Montana are not. Therefore, a business located in a remote location would be better served with a high availability configuration.

Hardware

QPC can supply hardware/software only and no services. Services are optional.

Services

QPC can provide services on a proactive flat-rate service contract for fixed scope items and then as needed escalation or break/fix support. We also do implementation and remediation services.

It should be noted that WatchGuard tech support is designed only for limited break/fix support. They do not provide configuration management, security consulting, or anything sophisticated. This is true of every network security appliance manufacturer. Security consulting will always be outside of the scope of tech support agreement between a customer and a manufacturer because security consulting is highly contextual and is an art form.

Rearchitect network

This is the work which needs to be done in order to correct the outstanding configuration issues.

- trusted network for office PCs
- an isolated VLAN for the POS system
- guest wireless
- trusted wireless
- WAP management isolated network to protect the WAPs
- Egress policies to protect trusted PCs, POS, and guest
- Configure cloud controller for WAPs
- Enroll WAPs and configure SSIDs
- Configure Total Security Suite
- requires Dave to participate in the configuration migration and provide a laptop with wireless and wired connectivity which can be remoted into with TeamViewer for the work

Project time is an estimate because we have not worked on the environment previously and do not have comprehensive knowledge of all of the environment components at this time. Time estimates provided are based upon the initial discovery call. (16 – 26 hours @ $195/hr)

Alternative configuration move and WAP only

The alternative is not recommended because it will not provide a result which utilizes the security subscription properly, nor resolves the network structure issues.

- existing configuration move without changes except to remove the gateway wireless controller configuration which would conflict with the cloud controller config
- no TSS implementation

- setup cloud controller for new WAPs
- enroll WAPs and configure SSIDs
- requires Dave to participate in the configuration migration and provide a laptop with wireless and wired connectivity which can be remoted into with TeamViewer for the work

Estimate up to 8 hours @ $195

Optional proactive management services

- Health and traffic monitoring
- Compliance reporting into QPC provided client compliance portal
- Fireware upgrades
- Configuration tuning after Fireware upgrades

$2400/yr/Firebox $300/yr/WAP

Pricing for recommended products

Item	Qty	Per unit	Extended
WatchGuard Firebox Trade-up T45-PoE w/ 3 year Total Security Suite	1	$1,910.80	$1,910.80
Premium RMA 3 year	1	$246.50	$246.50
AP130 WAP with 3 year license	2	$356.32	$712.64
Power Supply for AP130	1	$20.64	$20.64
Shipping	1	$14.00	$14.00
Total			$2,904.58

We only provided pricing on the T45-PoE here and not the T85 because it is most important that the business have budget to apply to secure configuration management. The T45-PoE is expected to be sufficient as specified earlier in this document. The T85 would be more expensive.

Product licensing is delivered via email to the designated email of the customer as provided prior to purchase. Physical product is shipped direct to customer at designated shipping address.

About

QPC has been a WatchGuard Gold partner since 2009, which is the highest level of technical certification level an organization can achieve with the manufacturer. QPC has five full-time certified engineers on staff. We have additional specializations & technical certifications in all other WatchGuard technologies as well as many other technologies.

https://www.qpcsecurity.com/certifications-and-partnerships/

https://www.watchguardmaster.com/