Cybersecurity Platinum Whitepaper

Introduction

Cybersecurity Platinum is a cybersecurity solution that provides a high level of security protection against threats, including malware and malicious actors, and mitigates vulnerabilities on imaging devices manufactured by Canon Medical Systems Corporation: https://us.medical.canon/ . Therefore Cybersecurity Gold lowers the attack surface by significantly lowering the risk. It is our highest recommendation that the Canon medical imaging equipment be isolated from the facilities network by the Cybersecurity Platinum offering.

Technical Summary

Cybersecurity Platinum consists of a firewall appliance, Barracuda F12: https://www.barracuda.com/products/cloudgenfirewall/models and InnerVision Plus. This proprietary configuration includes a VPN connection to Canon Medical Systems HQ that allows:

- Remote application and service mirroring of the imaging device (on applicable systems)
- Intrusion Prevention System (IPS) on traffic passed to/from the imaging device, as well as traffic on the facilities network destined for the Barracuda device
  - IPS updates are performed automatically from Canon Headquarters
- Canon customized reporting
- Syslog output to facilities Security Information and Event Management (SIEM) configurable to facilities discretion
- Protocol detection
- 360 Connect visibility allowing customers to view reports
- eWatch that consists of temperature/humidity monitoring and incoming power monitoring
- InnerVision Plus running on Windows 10 with automatic updates using WSUS located on the trusted side of the Barracuda device

VPN Summary

Cybersecurity Platinum supports four VPN methods:

a) Barracuda Firewall (Recommended)

- TINA VPN (DEFAULT) – a proprietary extension of the IPSec protocol developed to improve VPN connectivity and availability. REF: https://campus.barracuda.com/product/cloudgenfirewall/doc/72516595/tina-vpn-tunnels/. Initiated by the Canon Firewall and attached to the Canon medical imaging modality, VPN out-bound on tcp 691 (management tunnel) and 692 (data tunnel) to the Canon Service concentrator at 198.100.16.230.
- SSL/TLS (v1.2) VPN - Initiated by the Canon Firewall and attached to the Canon medical imaging modality, VPN out-bound on tcp 691 (management tunnel) and 692 (data tunnel) to the Canon Service concentrator at 198.100.16.230.
- IPSec (NAT-T) - Initiated by the Canon Firewall and attached to the Canon
- medical imaging modality, VPN out-bound on udp/500 (isakmp) & 4500 (NAT-T) to the Canon Service concentrator at 198.100.16.230.

b) Lan-to-Lan IPSec: VPN from customer's own VPN device to the CANON Service concentrator. Customer VPN must support IPSec NAT-T, and 1-to-1 NAT to prevent IP conflict. Customer is responsible for all access control and malware mitigation measures. Requirements include:

- The Canon Service VPN concentrator maintains a full time, bi-directional IPSec tunnel to the Customer concentrator with keep alive.
- Canon requires a IPSec PreShared Key with a minimum of 19 random characters.
- The Canon Service VPN network operates on a 172.17.0.0/16 address range. The Canon HQ servers and workstations use 172.17.1.0/24. Canon can SNAT this to 198.100.17.0/24 (public range owned by Canon) if desired.
- To prevent IP conflicts, Canon Service assigns each suite of modality equipment a 172.17.x.y/28 subnet as an alias. The customer system will need to DNAT to their actual IP's.
- Access to/from the VPN between the customer and Canon must be limited to Canon
- modality equipment ONLY, preferably by use of a VLAN.
- The Canon modality equipment must retain access to local PACS, DICOM Printers, MWM, 3-D Workstations, and other devices as required.
- • The Canon modality equipment must be configured for the above (routing, gateways, host tables etc.)

VPN Negotiation

- The Customer VPN System at Canon has a public IP address available on the internet.
- Capable of IPSec or SSL/TLS VPN out-bound (initiated from inside customer network outbound to Canon).
- Full time, bi-directional Site-to-Site VPN tunnel with keep alive.
- Authentication by Pre Shared Key for IPSec, or x.509 Digital Certificates for SSL/TLS VPN.
- NAT-Traversal capable (to allow traversing customer's masquerading firewall without need of in-bound open ports or dedicated global IP address.)

Tunnel Traffic

- Bi-directional - Low Bandwidth – High Security.
- Most common VPN traffic will be ICMP, Telnet, and small FTP packets between the
- Customer's Canon Medical imaging equipment and servers at Canon Headquarters.
- Remote servicing traffic from Canon Headquarters may include: FTP, Telnet, Ping, SSH, pcAnywhere, VNC, Dicom, and various proprietary ports (see Ports for specifics).
- If the recommended Barracuda Firewall method is used, this traffic is safely encapsulated all the way to the Canon medical imaging device(s).

Ports

- The only traffic allowed thru these VPN tunnels are ICMP and TCP ports 20, 21, 22, 23, 25, 80, 104, 177, 389, 443, 1053, 1099, 2025, 3025, 3389, 4025, 5025, 5631, 5016, 5900, 6025, 7025, 8025, 50001 (*this list is subject to adjustment). All others are DENIED.

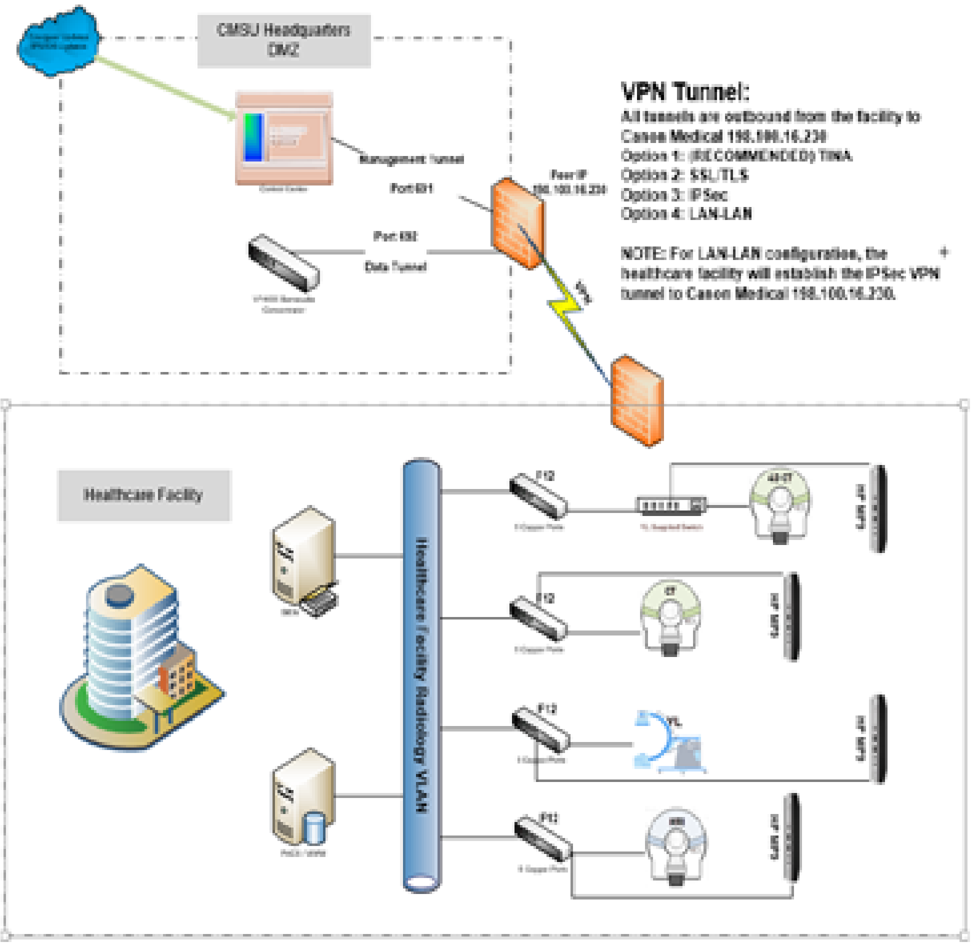
Security

- Any Canon employee attempting to access a customer's Canon medical imaging system must be authenticated by the Canon Active Directory which will grant permission to access specific customer's VPN tunnels. The Canon system allows this degree of granular control. The Canon Customer VPN system is separated from the Canon internal network by a series of firewalls. All Canon HQ servers and workstations are automatically updated for OS patches, malware and virus definitions, and IPS definitions.
- On rare occasions, customer's data, which may consist of Patient Health Information (PHI), may transverse the VPN. As a business associate, Canon takes high security precautions to protect this data. Data may consist of log files, DICOM images, and remote viewing of the Canon Imaging device. All Canon employees that have access to this data must follow specialized Canon security training on PHI and how to handle such data, including the proper destruction of that data. Data is only gathered when an issue occurs and never gathered for statistical purposes (unless a special signed agreement is in place). All data is stored temporarily only and is removed securely when the issue has been resolved. At NO time is data stored permanently at Canon Medical Systems.

Made For life

Audit trails are available on demand. All Canon employees must use two authentication in order to access a customer's VPN. These audit trails will include log in/out time and protocols used.

Architecture Drawing



VPN Tunnel:

All tunnels are outbound from the facility to Canon Medical 198.100.16.230
Option 1: (RECOMMENDED) TINA
Option 2: SSL/TLS
Option 3: IPSec
Option 4: LAN-LAN

NOTE: For LAN-LAN configuration, the healthcare facility will establish the IPSec VPN tunnel to Canon Medical 198.100.16.230.

CANON MEDICAL SYSTEMS USA, INC.
2441 Michelle Drive, Tustin CA 92780 | 800.421.1968

Made For life