CANON MEDICAL SYSTEMS USA, INC.

Remote Service and Support
VPN to Customer's Canon Medical Devices
(a white paper)

June 2019

Technical Summary

The Service Networking Support (SNS) Group at Canon has implemented a system to allow remote service and support via VPN connections to a Customer's Canon medical imaging devices. This system design supports the recommendations of the MITA division Security & Privacy Committee of NEMA (referenced below) by either of three connectivity methods.

This system has the following attributes:

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 Security: Canon Side for specifics).
- If the recommended Canon Firewall method is used, this traffic is safely encapsulated all the way to the Canon medical imaging device(s).

Security: Canon Side

Following the MITA recommendations, any Canon employee attempting to access a customer's Canon medical imaging systems 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 and virus definitions.

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: Customer Side

It is our highest recommendation that the Canon medical imaging equipment be isolated from the Customer network by a Canon Firewall, or else by a Customer configured VLAN. Many years of experience has shown these to be the surest mitigation of network malware.

Canon Medical Systems USA, Inc. Supports Three VPN Methods:

a) **Canon Firewall** (Recommended)
Depending on the Canon medical imaging system installed:
   i) **SSL/TLS (v1.2) VPN -** Initiated by the Canon Firewall and attached to the Canon medical imaging modality, VPN out-bound on tcp/443 to the Canon Service concentrator.
   ii) **IPSec** (NAT-T) **-** Initiated by the Canon Firewall and attached to the Canon medical imaging modality, VPN out-bound on udp/500 & 4500 to the Canon Service concentrator.

b) **Lan-to-Lan IPSec:** VPN from customer's own VPN device to the CANON Service concentrator (**NEMA "Solution A"**). 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.

Canon Firewall: By far the quickest, simplest, and most secure method. This isolates the Canon medical imaging equipment on the Customer network. We have found this to be the best form of malware protection. Canon provides, *free of charge to warranty and contract customers*, a specially configured firewall system that is placed with the medical imaging system. This firewall has the capability to initiate an outbound VPN tunnel to the Canon Service concentrator by either SSL/TLS VPN or IPSec. The customer IT department is allowed access the Canon Firewall.

Lan-to-Lan IPSec (**NEMA "Solution A"**)**:** Customers desiring to use their own VPN equipment are supported by this solution. However, experience has shown this to be the most time consuming, least stable and least secure method. The LAN-to-LAN IPSec VPN tunnel configuration usually requires IP NAT'ing and routing/ACL changes on the customer IT equipment. Network architecture for malware protection is the responsibility of the Customer.

PHI (Protected Health Information)

Most traffic sent across the Remote Service VPN connection does not include PHI. Normally only system performance or troubleshooting data is sent back to Canon.

Exceptions:

- Customer Imaging Technician invites Canon Support to connect via remote desktop making PHI visible.
- Generally, all data sent to Canon is anonymized. In certain cases, data required for troubleshooting purposes may inexorably contain PHI. Such data is retained only long enough to allow completion of support request and is only accessible by authorized Canon support personnel – in accordance with HIPAA as a Business Associate.
- The Customer has a Research Agreement with Canon that may require PHI.

Virus, Trojans, and Worms

Network-based malware has been a plague on the networking industry for decades. Many of newer medical imaging devices have been designed on Microsoft Windows platforms. However, a common misconception is that they are built using standard off-the-shelf software such as a common server might use. A medical imaging scanner, controlling ionizing radiation or high energy fields and patient motion, often utilize highly imbedded systems. Patient safety and diagnostic precision are paramount. When some new network threat is detected, and an OS patch is available, these must be thoroughly tested by the manufacture's engineering division prior to release. Just because a patch is available from Microsoft does not mean it is safe to use on a particular medical imaging device. Unfortunately, there can be considerable delays in release while these patches are tested and, if necessary, recompiled to operate correctly.

A well designed network environment is often all that is required to immediately protect a medical imaging scanner from such threats. Canon always recommends and provides *free of charge to warranty and service contract customers*, a Canon Firewall to isolate the Canon medical imaging device. The Canon Firewall has a state-full firewall feature that can lock down the Canon modality equipment tightly, and make it very difficult for malware to penetrate.

The medical imaging industry as a whole, through the MITA division of NEMA, is recommending standards for control of these issues. For more information regarding these industry standards please refer to the various white papers at:
http://www.medicalimaging.org/policy-and-positions/

Canon Firewall (Recommended)

Canon Medical Systems USA, Inc. now universally recommends the Canon Firewall as best method of malware mitigation and VPN connectivity. This device:
A) Acts a state-full firewall, permitting only authorized connections between the customer network and the modality equipment subnet. Only DICOM traffic, point-to-point and port-to-port, is allowed through. This has proven to be very effective against malware attack.
B) Initiates a VPN tunnel out-bound to the Canon Service Concentrator. This tunnel may be either IPSec NAT-T or SSL/TLS (v1.2) VPN depending on the system installed. No in-bound ports are required on the customer's internet firewall.

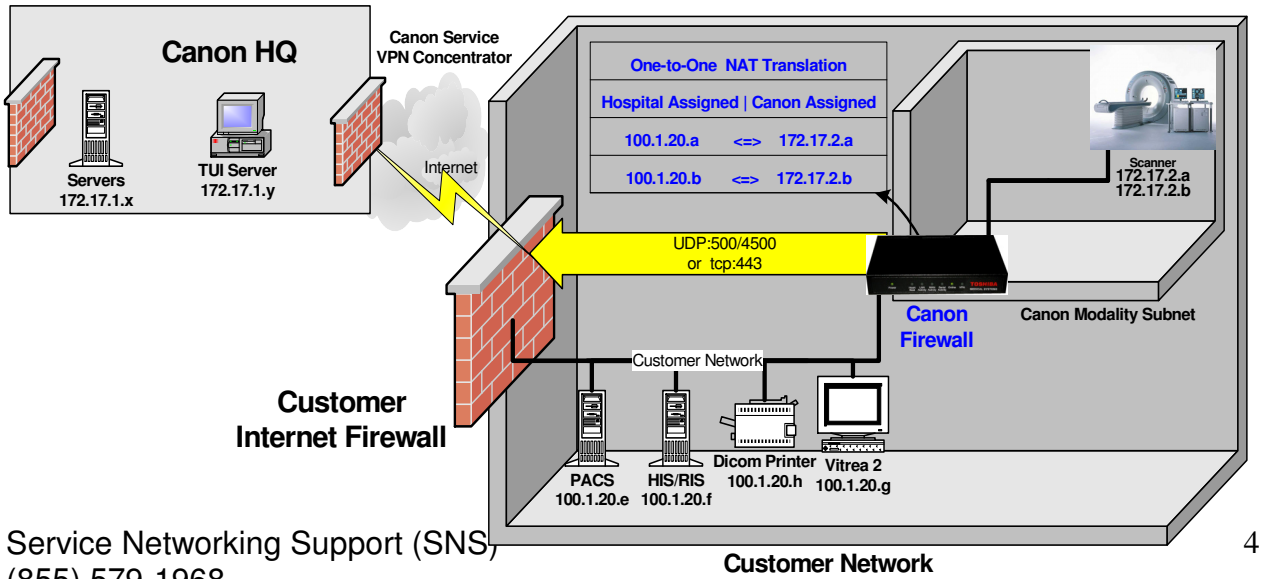
- The customer IT department is allowed access to the Canon Firewall.
- The customer IT department assigns (static) IP addresses to the Canon medical imaging equipment on their network. The Canon Firewall uses 1-to-1 NAT to ensure transparency.
- VPN connection is made using tcp-443 for SSL/TLS VPN, or udp-500/4500 for IPSec.
- Each suite of Canon medical imaging equipment is provided its own Canon Firewall.

Customer Side Configuration For Canon Firewall

- For **SSL/TLS VPN:** Allow tcp-443 (https) out-bound from the Canon Firewall to the Canon Service concentrator at 69.238.9.**16**. If a web filter or proxy is employed, an exemption is required for tcp/443 from the device to permit proper certificate handshaking.
- For **IPSec NAT-T VPN:** Allow udp-500 (isakmp) and udp-4500 (NAT-T) out-bound from the Canon Firewall to the Canon Service concentrator at 69.238.9.**15**.
    1. If the customer's network operates on routable addresses, rather than private addresses, then IP-Protocol 50 [ESP] may also be required.

Canon Service Department will require the following data:

- The customer's public IP peer address that the Canon Firewall's packets will be masqueraded as, and received from.
- A dedicated static IP address (same subnet as the modality system) for the Canon Firewall.
- The IP addresses and port numbers for each Customer DICOM device that the Canon modality devices send to (e.g. PACS, DICOM Printers, MWM etc.)



Lan-to-Lan IPSec VPN (Supported)

The MITA division of NEMA provides for an industry standard LAN-to-LAN IPSec VPN structure between medical imaging vendors and HIPAA regulated health care facilities.
Ref: http://www.medicalimaging.org/policy-and-positions/
Please use the above as the definitive references. The following text is the Canon Medical Systems USA, Inc. interpretation and implementation:

NEMA "Solution (A)" consists of a Site-to-Site IPSec VPN tunnel between the RSC (Remote Service Center) and HCF (Health Care Facility). All VPN connections from RSCs to the HCF would enter through a single point (HCF VPN Concentrator) and then be routed to the appropriate vendor equipment. As long as IPv4 is prominent, IP address conflicts between RSCs and HCFs are an issue that will require the use of 1-to-1 NAT'ing. Additionally, VLANs, ACLs and routing rules may be needed for a secure implementation.

Requirements For NEMA "Solution (A)" Connection To Canon:

- 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.)