Delivering a Secure Network

National Intelligence-Grade Network Security Solution

QNS and Critical Infrastructure Networks

Industrial control systems, SCADA networks, banks and payment networks, and the like can deploy the QNS solution to protect new and existing devices, business, and services. The QNS solution will secure data in transit, protect precious and personal data, prevent all unauthorized network access, and ameliorate DDoS, MITM, and other nefarious network activities.

QNS achieves superior security through a hardware security barrier that incorporates a True Random Number Generator (TRNG) delivering up to one million keys per second to enable packet-level encryption, where each packet or transaction can have a unique and truly random key (think DUKPT). Key entropy is continuously monitored for assurance. This permits industry-leading, secure communications anywhere, even when utilizing public links including LTE and the Internet. The QNS approach removes all opportunities for either man or machine to ever discover a security key, thus, thwarting internal exploits as well as remote attacks.

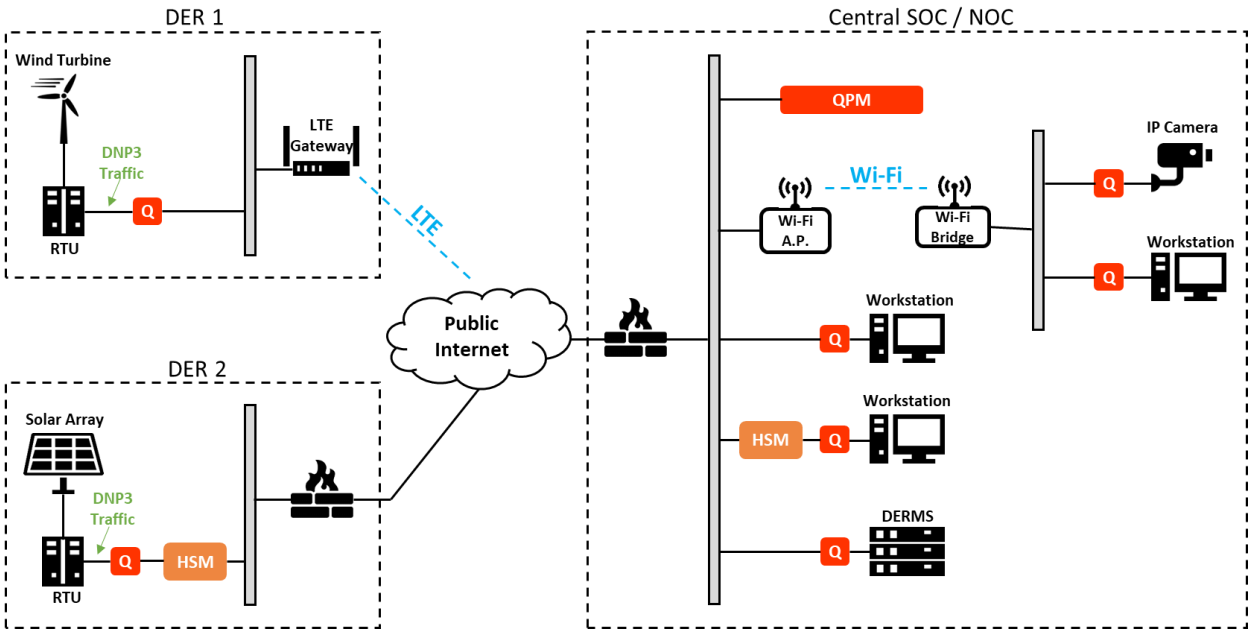

Figure 1. Power Grid, ICS, or Financial Network Implementation Schematic

Introduction to Q-Net Security

QNS provides the strongest commercially-available cybersecurity network solutions for the protection of endpoints and data traveling over networks supported by both private and public infrastructure. The hardware-based systems deliver quantum compute-resistant security that incorporates aspects of a distributed firewall, sessionless VPN, and infinite one-time pad yet is drop-in easy to implement without disruption or modification of existing endpoints, simple to manage, designed to lower network operating costs, and engineered to last for decades without updates.

This hardware-based solution offers superior security, yet it is fast and easy to deploy. The in-line hardware I/O elements (QIOs) are small devices that secure precious data flowing between every endpoint in a network. Complete security is built directly into each QIO's silicon. Creating security directly in silicon avoids the use of vulnerable software and/or Operating Systems which are stored program-based, i.e., general-purpose processors, often requiring frequent updates to patch newly discovered security holes.

At the heart of the hardware-enabled solution is AES encryption (using 256-bit keys) and a novel symmetric Just-in-time Key (JitKey) distribution that can provide a unique random key for each packet. The keys are not discoverable by man or machine and require no active key management. There are no secret algorithms; everything about the QIO is assumed to be public knowledge yet the chances of cracking a JitKey packet are infinitesimal and compromising a single data packet provides no information to assist in cracking the next. While each packet is encrypted using different keys, transmission efficiency is very high (greater than 97%).

Command and control of the secure network is handled by the QNS Policy Manager (QPM), which can be deployed in a single production point of presence. The QPM securely communicates to each deployed QIO, sets up initial communication between allowed secured endpoints, and then continues in a monitoring roll. While the QPM provides the ability to set up, monitor, and control each secure endpoint, no secure user data ever flows through the QPM. Thus, end-to-end security is always maintained.

High availability can be assured through redundancy of the QPM, the network, and the QIOs. The QNS solution drops into legacy networks installing easily and quickly. There is no need for the installation of additional software on any of the protected devices. This can even be implemented in active networks without need to bring the entire network down. This capability creates migration strategies for high-security networks that were previously unavailable.

This hardware-based approach provides many advantages over traditional software-based solutions including:

- Internally-generated random keys that change every transaction
- Line-rate operation
- Seamless operation with existing infrastructure and endpoints

The QNS solution is purpose-built to create an impenetrable barrier between defined endpoints and all remote attackers. QNS is national intelligence-grade, quantum compute-resistant security that is more powerful than any other cybersecurity solution in the world and is suited to drop into active networks.

Additional Detail

All traffic into and out of a QNS-secured endpoint can only originate from and go to another endpoint within the secure network (i.e., protected by a QIO). Any spurious or malicious traffic from outside the secure network will be rejected by the QIO and will not enter the networked systems. This includes malware and any other external attack vectors. Since all traffic within the network will be secured using the QNS JitKey (securing each packet with a different TRNG-generated key) any traffic that should leak out, even under the direction of a malware agent, will be uncrackable rendering it useless. Therefore, in most applications, customers are assured of high security without the need for antivirus software. Also, because the QIOs have no IP addresses, they are invisible to attackers and pen testing will only disclose that the protected endpoint device is secure. Thus, despite an attacker's exploits, the QNS hardware cannot be penetrated and will stay intact and secure.

In general, systems working entirely within a QNS secured network do not need, and will be more secure than, conventional malware software. Existing deployed endpoints can be tightly secured without changing the internal system components; the computers and devices inside can continue to use their existing operating systems (such as Windows CE or Windows XP) and software applications so that the endpoint can be secured without first having to upgrade the system.

Man-in-the-Middle (MITM)

When unauthorized data are sent to one of the protected endpoints, as would be the case for a man-in-the-middle attack, the data are dropped and do NOT make it through the QIO hardware barrier to the endpoint. This critical operation fully protects the endpoint system; no unauthorized data will enter the secured system even when directed by a MITM or while under DDoS attack (an aggressive attack, which overloads the network and often blocks the arrival of all data). With QNS protection authorized flows will resume once the attack stops. Note that an endpoint secured with QNS will be unable to send data out to any unauthorized endpoint, thereby preventing a malware-infected machine from attempting to "call home" to receive nefarious instructions or to send precious data.

Malware

A QNS implementation will effectively reduce the extent to which malware may impact a network by:

1. reducing the attack surface (it can only propagate to another system that is pre-authorized);
2. removing the ability to receive control signals from an outside source; and
3. stopping data and information from leaving the Q-Net.

If, through human error, malware inhabits a protected endpoint, QNS will only allow that malware or nefarious information to be transmitted between allowed nodes within the Q-Net. The efficacy of the malware is also dramatically reduced if not thwarted altogether as most malware needs instructions from a distant system to be activated; QNS stands guard and will not allow these instructions to reach the endpoint. And even if a QNS-protected system contains malware, the afflicted system cannot transmit precious data (such as credit card numbers, names, or telemetry) to a remote system. With the malware control hampered and attack surface diminished, this will provide additional time to detect and remediate malware that has made its way into a network.

HSM Comparison

The QNS solution is superior to any software-based systems in the market, including routers enabled with encryption and employing HSMs (most HSMs *are* software). At its core, QNS does not use standard processors, kernels, or software but instead uses a fixed, special purpose hardware-based solution that performs only high-security functions. This system cannot be altered, cannot be seen by an adversary as it does not have an IP address, and uses AES-256-GCM, a special form of AES authentication designed for non-repudiation. The endpoints that QNS protects do not need to be changed, modified, or updated, as they require no agents to be deployed. Keys are not available to any human or machine at any time and do not need to be managed externally; the hardware purposefully manages the keys and keys will change per packet or transaction.

MPLS Compatibility

The QNS Security solution is compatible with all manner of network protocols including MPLS. QNS secures only the payload and does not modify the header and routing information so that all network protocols, including MPLS, work seamlessly. N.B.: QNS is strong enough to use public network links effectively, enabling network cost savings.

VOIP

QNS works seamlessly with all forms of data, including files, streams, video, and voice. The minimal network overhead and low latency of QNS mean that VOIP will not experience any performance degradation and user experience will be uncompromised.

Quantum Compute-resistant Cybersecurity

The US National Institute of Standards and Technology (NIST) encryption standard, AES-256-GCM, uses 256-bit keys. A conventional brute-force attack would take, on average, 2^{255} trials to discover the correct key. That is a dauntingly big number corresponding, in decimal notation, to five followed by 76 zeroes, just a little less than the current estimate of the number of atoms in the universe. Using today's computers this is clearly a computationally infeasible number of trials. Tomorrow's computers may provide a dramatic increase in computational power by use of certain quantum-mechanical phenomena. Only extremely primitive quantum computers exist today, but their potential to accelerate a brute-force search or an integer factorization should not be discounted. Fortunately, QNS technology is quantum compute-resistant because it uses no encryption algorithms based on integer factorization such as used in a classic public-key infrastructure. Also, Grover's algorithm running on a quantum computer promises the equivalent of 2^{128} trials for discovery of an AES-256 key, still a computationally infeasible number of trials. In fact, it corresponds to more than a billion-billion computers each with a 10-gigahertz clock-rate computing for the age of the universe. A recent report published by the National Academies suggests a hypothetical quantum computer would take over a trillion years to break this encryption; and with QNS a criminal would be required to perform this set of computations every microsecond! Thus, QNS technology has been deemed to be quantum compute-resistant.

Remote Attack Cybersecurity

Attacks initiated from an untrusted-network endpoint will take advantage of the stored-program nature of all modern computers. The attacker finds a way to insert a snippet of malicious code into the target computer. From this beachhead the attacker can freely explore and modify the target's data and instructions. Such remote attacks are difficult to prevent in today's complex and fluid software

environments because of the attacker's many ingenious methods for corrupting a target computer's programs. QNS technology eliminates this opportunity for the attacker. QNS technology stores no instructions in read/write memory, offering no way to insert or modify a QIO's actions to achieve a successful remote attack.

Physical Security

Whether it be contained in a separate device, attached to an endpoint, or integrated into an endpoint's hardware, a QNS input/output unit can be stolen. Using that stolen unit to access a Q-Net would, however, require that it be declared trustworthy and (re-)enrolled into the targeted Q-Net. Only a trusted individual can carry out these operations. The absence of an errant unit from a Q-Net is almost certain to be discovered by the QNS Policy Manager before or during re-enrollment. Since the functionality of these units is expressed in silicon, no useful modification to a unit is possible. The examination of a stolen unit is also fruitless since the only useful information contained therein is the unique shared secret and no hardware access path to it exists. If a future process (likely involving an extremely tedious method and highly expensive laboratory equipment) was able to reveal the shared secret, even then no other Q-Net information would be in jeopardy; the theft will certainly have been discovered quickly and the shared secret purged before any damage could be done as the Policy Manager is alerted immediately when a device is disconnected.

IPsec and SSH/TLS

Many interconnected systems can communicate using encrypted packet payloads. This is most frequently implemented using software and processing resources on the endpoint. As such, this raises several important operational and security challenges, some of which are outline here.

As with any general-purpose processing solution, IPsec demands constant care and effort in updating the OS, kernel, and application software as potential compromises are discovered. Management of these processes can be tedious and expensive, especially when there are a heterogeneous set of endpoints. Further, as is the case in many control systems and IoT applications, the endpoints are often not managed or easily updated by the implementing organization. For example, this may result from organizational structure limitations, a mixture of hardware manufacturers and software versions, or tightly integrated vendor services.

It should be noted that any updated software systems can, by design, be altered or changed, even by an adversary. And as many of the endpoints were not designed with security processing in mind, application performance and troublesome latencies are often observed in practice.

IPsec and SSH/TLS implementations leverage an initial key exchange which defines the secure session during which data are transferred. This requires global management of these system keys and certificates. Session keys are established between the endpoints. These keys are usually used for the duration of the session which can last for hours or days. Several compromises have been identified with this process especially with poor implementations of the initial Internet Key Exchange (IKE) process. As discussed in the man-in-the-middle (MITM) section, MITM attacks are difficult to prevent for software implementations and have been used to compromise IPsec implementations as well. One such activity was documented in an article in February of 2019, in which IKEv2 is compromised revealing IPsec tunnels to be insecure.

With a QNS solution there is no conventional session key, no external key management or cert server, and no PKI exchange of session keys. Only fully symmetric keys are securely distributed and can be changed as frequently as a million times per second using a true random number generator (non-algorithmic bit sequence producer). Attempting to stand in the middle of the flow to discover the keys is pointless. And since the QNS solution is in immutable hardware, it cannot be compromised within an application stack or using operating system weaknesses (there is no kernel, OS, or application software).

The QNS solution also provides fine-grained endpoint security definition (essentially firewalling rules). This means that should the software of an endpoint become compromised, it can only send packets to those endpoints already allowed; it cannot force the Q-Net endpoints to accept data, nor receive data from or send data to unauthorized endpoints. As most malware requires an external signal to activate an attack and often seeks data exfiltration, such actions are stopped dramatically lessening the impact made by a compromised endpoint. N.B.: while there is the potential for an endpoint itself to be compromised, a Q-Net IO device attached to that endpoint can NEVER be compromised, today or any time in the foreseeable future.

Summary

QNS solutions work seamlessly with existing network and enterprise infrastructure; we don't replace it, complicate it, or degrade its performance. Instead, we simply lay QNS on top of your current network to create an impenetrable network segment where defined endpoints can communicate with ultimate protection and confidence.

Customer Remarks Highlighting QNS Value

Future-proof strong security for today

- Per-transaction true random key (DUKPT)
- Complies with NIST/NSA standards for quantum computing-resistant encryption

Thwarts most cyberattacks

- Prevents anyone sending in control messages or sending out precious data
- Eliminates system compromise from phishing attacks
- Protects against jackpotting (e.g., Cobalt, Ploutus.D, Peralta)

Creates an impenetrable shield even in antiquated systems

- Drop-in ready for use in existing public networks
- Easy to install and manage – even for field technicians
- Removes the need to modify OS, drivers, and application code currently in place (including Windows CE and XP implementations)
- Circumvents the need for security patches
- Relaxes anti-virus requirements
- Avoids external key management
- Rugged enough to be outside (no fans or moving parts)
- Alerts the SOC if the system is physically attacked

Cost-effective solution

- Costs less than a new HSM
- Designed to remain in place for decades without updates
- Reduces system maintenance costs
- Assists with PCI-DSS compliance