Barracuda
Your journey, secured.

Secure connectivity for industrial internet of things and networked industrial machines

with Barracuda Secure Connector and Barracuda CloudGen Firewall

WHITE PAPER

NETWORK AND APP SECURITY

The world's getting connected

The term "the Internet of things" was coined by Kevin Ashton of Procter & Gamble in 1999. "Things", in the IoT sense, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, cameras streaming live feeds, or automobiles with built-in sensors. Ashton correctly foresaw a world in which large numbers of connected things would communicate with each other autonomously via the internet—effectively creating an internet of things that is distinct from the internet of people.

Today we see a proliferation of smart, internet-connected home devices such as for control and automation of lighting, heating, ventilation, air conditioning systems, and appliances such as washer/dryers, robotic vacuums, air purifiers, ovens, or refrigerators/freezers that use Wi-Fi for remote monitoring.

In addition, we see an industrial internet of things (IIoT) and machine-to-machine (M2M), terms used for the industrial field of IoT where intelligent systems connect machinery, sensors, and control systems to enable rapid manufacturing of new products, dynamic response to product demands, and real-time optimization of manufacturing production and supply chain networks. Automated process controls, operator tools, and service information systems optimize plant safety, while security and asset management use predictive maintenance to maximize reliability.

IoT is an expanding market. According to Forbes the business-to-business spending on IoT technologies, apps, and solutions will reach $267B (€250B) by 2020. About fifty percent of that will be driven by discrete manufacturing, transportation and logistics, and utilities. Gartner indicates the market for IoT devices is poised to explode and will reach nearly 20.8 billion connected devices by 2020.

How to handle thousands of "things"?

Concerns have been raised that the internet of things is being developed too rapidly, without appropriate consideration of the profound security challenges involved. Whereas traditional cyber criminals target information and financial assets, hackers exploiting vulnerabilities in the internet of things—which may include everything from ATMs and cargo ships to power plants and your pacemaker—will be able to cause real-world mayhem far beyond what a data breach might accomplish.

Most of the technical security issues are similar to those of conventional servers, workstations, and smartphones. This means that every "thing" needs a firewall for protection. Without a firewall, these connected devices easily become a target for cyber criminals. They can use the devices as bots for a DDoS attack, or infiltrate your network for other reasons. But how to handle the deployment and management of thousands of firewalls? What about the cost of such extremely large deployments?

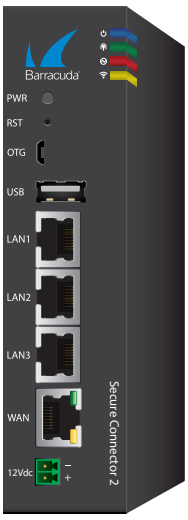
The IoT is also changing the way we work and collaborate. In the decade following 2000, many business planners sought to reduce costs and focus resources on their core business by outsourcing IT. Today, however, many of these planners are noting that the core business is directly integrated with IT—that operations and IT are no longer separable. They need to be connected, and suppliers, partners, and service providers also need to become part of these networks. All of this requires the definition of new roles and workflows with shared responsibilities. Who takes care of which components, what maintenance processes needs to be followed, and who are the decision makers?

Barracuda Secure Connector for the industrial internet of things

Consumer IoT devices like wearables and toys need to be secure by design. Barracuda offers solutions for professional IoT devices, for example smart meters and traffic lights.

The Barracuda solution consists of three components:

Barracuda Secure Connector establishes an encrypted connection between IoT devices and the machine access security broker, using Barracuda's proprietary enhanced IPsec protocol TINA, which is more resilient and provides better performance than most competitive VPN solutions.



Secure Connector appliance

The Secure Connector appliance comes with a choice of uplinks and automated failover in case one uplink fails. Besides wired uplinks typically use DHCP or static IP, the integrated WiFi can be operated in client mode to access the WAN via existing wireless networks. Secure connector models with integrated 4G/LTE modem offer even greater deployment flexibility. The Secure Connector appliance also provides centrally manageable edge computing support via built-in linux container. This lets you create custom control and monitoring logic for the devices protected by Secure Connector.

Ultra-compact design and affordable price point of the Secure Connector makes it flexible and easy to deploy across large IoT networks.

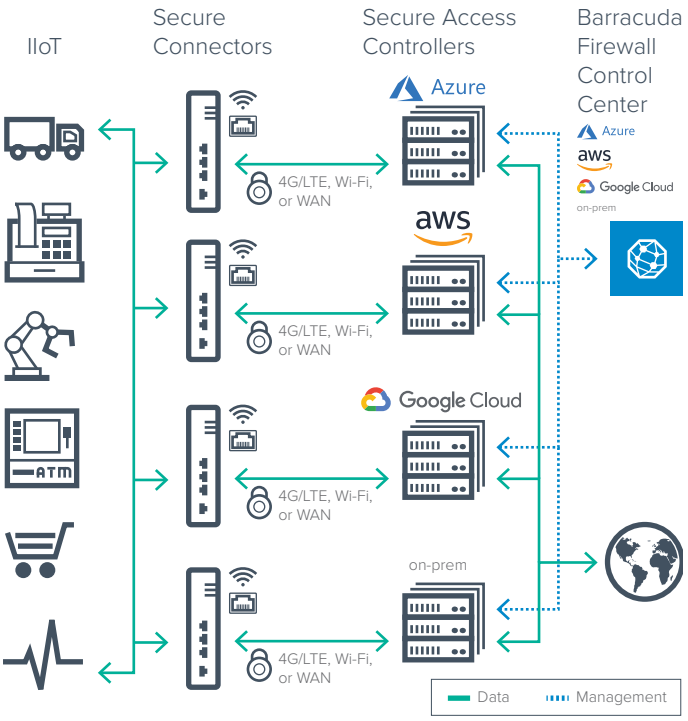
The **Secure Access Controller** acts as a connectivity hub for up to 2,500 Secure Connector appliances. It enforces security policies with the full feature set of Barracuda CloudGen Firewalls, including IPS, denial of service protection, application control, URL filtering, virus scanning, industrial protocol detection and enforcement, and even advanced threat protection, including CPU-emulation sandboxing.

Secure Access Controller is available as a virtual solution and can be deployed on-premises or directly in Microsoft Azure, Amazon Web Services, or Google Cloud Platform.

The **Barracuda Firewall Control Center** enables centralized management and secure remote connectivity for tens of thousands of IIoT devices from a single pane of glass.

When you need to manage a quick rollout across multiple remote locations—many of which may lack qualified IT personnel—the zero-touch deployment capabilities make it easy. Secure Connector appliances are shipped directly to the remote locations without the need for pre-configuration. Onsite personnel simply unpack the appliances and power them up. They automatically connect to the customer-owned Firewall Control Center, which sends full configuration settings to the appliances via an encrypted VPN tunnel. With no onsite IT expertise, the appliances become part of the security infrastructure. With zero-touch deployment, rollouts to hundreds and even thousands of remote locations are executed quickly and managed easily, and require far fewer IT resources.

Managing and maintaining security appliance configurations can be a complicated and time-consuming task. Barracuda uses a template-based configuration that lets you create templates at the various organizational levels supported by Firewall Control Center. Once a template is changed, all Secure Connector appliances linked to this template will automatically update within seconds.



Securing IIoT architecture

Barracuda CloudGen Firewall for industrial environments

This increase in connectivity also exposes formerly isolated systems, including large industrial control systems, to the dangers inherent in the internet. Barracuda offers advanced security solutions for big devices in industrial environments.

Authentication and segmentation for industrial components

The first step in securing these systems is to define effective perimeters between a secure, controlled realm and the world outside. These perimeters might be located deep within companies and manufacturing plants, but logically they are necessary. The most important element is to correctly determine where to place your perimeters.

In this process, you may create a large number of new perimeters, all of which need to be protected by a firewall. A solution with high scalability and easy manageability in that situation is critical to ongoing operational security.

Your firewalls also let you enforce new or existing access policies, so that technicians can access only the parts of the network relevant to their jobs, for example. Strong authentication techniques are critical to success in this regard, and it is typically considered a basic requirement of industrial security.

Detection and containment of threats

If your firewalls are correctly configured and deployed to defend the right perimeters, you will be able to detect and block threats and attacks. Even if a modern worm like WannaCry penetrates one area, it cannot spread throughout your infrastructure.

In designing your infrastructure, It is important to resist the temptation to cut down on firewalls by combining zones that should ideally be kept discrete, perhaps in order to simplify and centralize remote access. Within the protected domain, the primary objective is to make it impossible for an attack or advanced threat to spread across logical zones. This objective is what determines the number of firewalls and the shapes of the perimeters to defend.

Analysis of industrial protocols

Machine-to-machine communication uses a variety of familiar protocols, but also many protocols that are little known in the office IT world. Some of them are partly or fully proprietary and cannot be easily analysed. So, IIoT and OT security requires the flexibility to customize highly granular policies, including the ability to create your own protection profile patterns. It is, however, a process decision between IT and OT experts, what level of granularity fits into the protection profile.

For more detailed information on supported industrial protocols, please see Appendix “Supported industrial protocols” on page 7.

Joint operations between IT and OT

Until recently, the firewall was strictly an IT responsibility. However, OT security means introducing firewalls into places and processes governed by operations, most of them older than firewall technology itself. This makes it crucial for IT and OT leaders to commit to open collaboration.

The firewall in an industrial machine must be understood both as an integral part of IT’s network of firewalls, and as an integral operating part of OT’s network of machines. Both IT and OT must be flexible about change and lifecycle management to succeed with this model.

Secure remote access in industrial environments

Whereas the number one threat vector in the internet of people is email, in industrial control systems it is remote management access. Most design paradigms do not allow for remote access outside certain narrow environments. CloudGen Firewall’s Remote Access feature makes it extremely convenient to grant secure, temporary VPN access to sensitive parts of manufacturing assets for third-party-maintenance providers, providing a more secure alternative to the native remote management interface.

Your IT admin can configure granular permissions to let specified Operations staff open a predefined remote VPN connection, and authorize a third party to use it, via phone or tablet. Onsite Operations staff need no IT expertise.

Grant remote access to specific deployments via an app

Firewalls in harsh environments

Barracuda offers a range of specialized full-featured and ruggedized appliances with extended temperature range, shock resistance, and no need for active cooling. They are specifically designed for industrial control systems (ICS) used in critical infrastructure and for manufacturing industries in harsh environments, where networking equipment is exposed to extreme temperatures, humidity, dust, and vibration.

Centralized management with the Firewall Control Center fully integrates the rugged appliances in a large and dispersed ICS network.

Barracuda CloudGen Firewall F183R, front and top view

Barracuda CloudGen Firewall feature set at a glance

Barracuda provides all the connectivity and security features required to set up and run a dispersed OT network.

- Secure SD-WAN and traffic intelligence
- WAN compression
- Failover and link balancing
- Dynamic bandwidth detection
- Dynamic latency detection
- Performance-based transport selection
- Adaptive session balancing across multiple transports of a VPN tunnel
- Adaptive bandwidth reservation
- Application-based routing
- Application control
- Deep application context
- File content enforcement
- Custom application awareness
- User identity awareness
- Web filtering
- Botnet and spyware protection
- Intrusion detection & prevention
- DoS and DDoS protection
- Malware protection
- Advanced threat protection

Scalability, enhanced security, and comprehensive manageability

Barracuda solutions bring together scalability, secure and reliable connectivity, state-of-the-art security, and simple centralized management. The compact Secure Connector appliance is optimized for securing and connecting large networks of IIoT devices, easily and economically. A streamlined rollout process with zero-touch deployment and centralized management help keep your IT overhead low, and features like remote access help to establish collaboration between information technology and operational technology.

Flexible deployment options—appliances or virtual solutions on premises and cloud-native versions for Microsoft Azure and Amazon Web Services—give you the tools you need to implement a tailor-made architecture that matches your specific requirements, today and in the future.

Conclusion

According to Gartner, there will be nearly 20.8 billion devices on the Internet of Things by 2020. Network control and management of manufacturing equipment, asset and situation management, or manufacturing process control brings IIoT within the realm of industrial applications.

Whereas the realm of tiny IoT devices like wearables and toys will have to rely on security by design, many use cases can and must be approached with a new type of firewalling. Barracuda is addressing this challenge with an ultra-small appliance providing zone-based firewalling, which reliably connects each remote device with a Secure Access Controller, for intrusion prevention (IPS), antivirus protection, and application detection and control.

The digital transformation in today's manufacturing processes requires permanent and on-demand connectivity with customers, partners, and suppliers on a rapidly increasing scale. The challenge is to find the appropriate mechanism to securely connect OT (operational technology) with IT (information technology) and to manage this process, not only in scale, but also regarding shared responsibilities. Barracuda addresses this challenge with specialized full-featured ruggedized appliances and comprehensive centralized management.

Appendix “Supported industrial protocols”

For a complete overview on support industrial protocols, please see Barracuda’s online application explorer:
https://campus.barracuda.com/product/cloudgenfirewall/browse/application-explorer

S7 sub-protocols:

- Ack
- Alarm-8Indication
- Alarm-8Lock
- Alarm-8Unlock
- AlarmAck
- AlarmAckIndication
- AlarmLockIndication
- AlarmQuery
- Alarm-SIndication
- Alarm-SQIndication
- AlarmUnlockIndication
- Comm(legacy)
- CPUServices
- CyclicDataDB
- CyclicDataMemory
- CyclicDataUnsubscribe
- DiagnosticMessage
- Download
- Erase
- Forces
- GetBlockInfo
- ListBlocks
- ListBlocksofGivenType
- MessageService
- Notify-8Indication
- NotifyIndication
- Other
- PBCBSend/BRecv
- PLCControl
- PLCPassword
- PLCStop
- Read
- ReadClock
- ReadDiagnosticData
- ReadSZL
- RemoveDiagnosticData
- Request/Response
- RequestDiagnosticData
- Run
- ScanIndication
- ServerControl
- SetClock
- SetupCommunication
- Stop
- Upload
- UserData
- UserData-BlockFunctions
- UserData-CPUFunctions
- UserData-CyclicData
- UserData-ModeTransition
- UserData-OtherFunctions
- UserData-ProgrammerCommands
- UserData-TimeFunctions
- VariableTable
- WarmRestart
- Write

IEC 60870-5-104 sub-protocols:

- ACK File - ACK Section
- Bitstring of 32 Bit
- Bitstring of 32 Bits
- Bitstring of 32 Bits with Time Tag
- Bitstring of 32 Bits with Time Tag
- Call Directory, Select File, Call File, Call Section
- Counter Interrogation Command
- Delay Acquisition Command
- Directory
- Double Command
- Double Command with Time Tag
- Double-Point Information
- Double-Point Information with Time Tag
- End of Initialization
- Event of Protection Equipment with Time Tag
- File Ready
- File Transfer
- Integrated Totals
- Integrated Totals with Time Tag
- Interrogation Command
- Measured Value - Normalized
- Measured Value - Normalized Value with Time Tag
- Measured Value - Normalized Value without Quality Descriptor
- Measured Value - Scaled
- Measured Value - Scaled Value with Time Tag
- Measured Value - Short Floating Point Number
- Measured Value - Short Floating Point Number with Time Tag
- Packed Output Circuit Information of Protection Equipment with Time Tag
- Packed Single-Point Information with Status Change Detection
- Packed Start Events of Protection Equipment with Time Tag
- Parameter Activation
- Parameter in Control Direction
- Parameter of Measured Value - Normalized Value
- Parameter of Measured Value - Scaled Value
- Parameter of Measured Value - Short Floating Point Number
- Process Information in Control Direction
- Process Information in Monitoring Direction
- Query Log - Request Archive File
- Read Command
- Regulating Step Command
- Regulating Step Command with Time Tag
- Reset Process Command
- Section Ready
- Segment
- Set Point Command - Normalized Value
- Set Point Command - Normalized Value with Time Tag
- Set Point Command - Scaled Value
- Set Point Command - Scaled Value with Time Tag
- Set Point Command - Short Floating - Point Number with Time Tag
- Set Point Command - Short Floating Point Number
- Single Command
- Single Command with Time Tag
- Single-Point Information
- Single-Point Information with Time Tag
- Step Position Information
- Step Position Information with Time Tag
- System Information in Control Direction
- System Information in Monitoring Direction
- Test Command with Time Tag

IEC 61850 sub-protocols:

- General
- Goose
- MMS
- SMV

MODBUS sub-protocols:

- (legacy)
- CAN-Open General Reference
- Data Access
- Diagnostic Check
- Diagnostics
- Encapsulated Interface Transport
- File Access
- Get Communication Event Counter
- Get Communication Event Log
- Mask Write Register
- Read Coils
- Read Device Identification
- Read Discrete Inputs
- Read Exception Status
- Read FIFO Queue
- Read File Record
- Read Holding Registers
- Read Input Register
- Read/Write Multiple Registers
- Report Server ID
- Write File Record
- Write Multiple Coils
- Write Multiple Registers
- Write Single Coil
- Write Single Register

DNP3 sub-protocols:

- Abort File
- Activate Configuration
- Application Control
- Assign Class
- Authenticate File
- Authentication Error
- Authentication Request
- Authentication Response
- Close File
- Cold Restart
- Configuration
- Confirm
- Control Functions
- Delay Measurement
- Delete File
- Direct Operate
- Direct Operate no ACK
- Disable Spontaneous Messages
- Enable Spontaneous Messages
- File Access
- Freeze and Clear
- Freeze and Clear no ACK
- Freeze Functions
- Freeze with Time
- Freeze with Time no ACK
- Get File Info
- Immediate Freeze
- Immediate Freeze no ACK
- Initialize Application
- Initialize Data
- Open File
- Operate
- Other
- Read
- Record Current Time
- Response
- Response Messages
- Save Configuration
- Select
- Start Application
- Stop Application
- Time Synchronization
- Transfer Functions
- Unsolicited Response
- Warm Restart
- Write

Barracuda®
Your journey, secured.