Extending Cisco ISE to IoT and Public Clouds

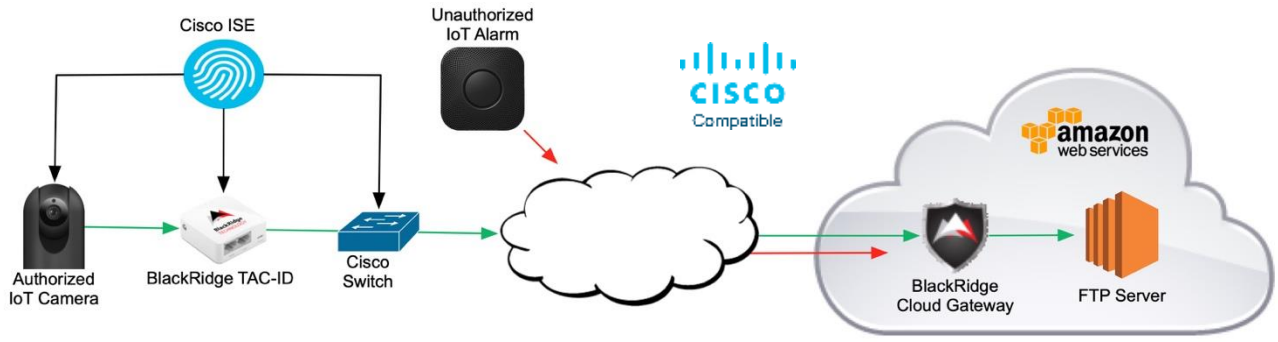
Addressing the Security Challenge at the Convergence of Information and Operational Technology Worlds

New digital services and connected Internet of Things (IoT) devices continue to be at high risk from security breaches and the subsequent impacts to consumer privacy and even personal safety. The challenge of securing industrial control systems (ICS) and other critical infrastructure devices and systems can be addressed with the BlackRidge Transport Access Control (TAC) product line. BlackRidge TAC lets organizations establish end-to-end trust by transporting identity through the stack – across already installed IP Connected sensors to clouds and gateways – both cost-effectively and with minimal latency added to the network.

BlackRidge can extend Cisco Identity Services Engine (ISE) from physical on-premise enterprise Information Technology (IT) or Operational Technology (OT) networks to cloud or hybrid deployments, stopping cyber-attacks and insider threats by allowing only identified and authorized users and devices to connect to the platform. As a Cisco Preferred Solution Partner, BlackRidge certified products are listed in the Cisco Solution Marketplace, the premier online exchange for networking solutions.

How it Works

In order to extend Cisco ISE and TrustSec functionality to the cloud, a BlackRidge cloud gateway and TAC Identity device (TAC-ID) are deployed to secure the end-to-end communications for IoT or OT devices. Provision of existing IoT devices is handled by Cisco ISE. Furthermore, ISE certificate authority also is used to provision an X.509v3 certificate to the TAC-ID. The TAC-ID will use this to insert identity to the devices connected to it. In this example, in the AWS Cloud an FTP server is deployed as a virtual resource for IoT devices, and this resource needs to be protected from malicious access. The BlackRidge Cloud gateway will only allow access to establish sessions that have an authenticated identity. The use of TAC-ID ensures that the remote device does not need to "log in" to authenticate. The BlackRidge Cloud Gateway intercepts incoming traffic destined for the FTP server and will only forward traffic from authorized IT and OT devices. All other traffic will be stopped and discarded by the AWS Gateway, effectively making the FTP server invisible to any unauthorized entity.



Extending Cisco ISE to IoT and Public Clouds

IoT Device to FTP Server Authentication Breakdown

1. The IoT device is connected to the Trusted port of the TAC-ID. The Untrusted port of the TAC-ID is then connected to any network that faces the outside internet. Since the BlackRidge TAC-ID solution lives entirely on the TAC-ID device itself, no further configuration or client installation is needed on the IoT device.

2. When the IoT device initiates a connection to the FTP server in an AWS Cloud the TAC-ID, which has a pre-installed X.509v3 certificate, presents this certificate to the BlackRidge Cloud Gateway protecting the FTP server. The AWS Cloud Gateway compares the TAC-ID's certificate with its own database of known certificates. If there is a match, the BlackRidge Cloud Gateway creates an identity for the TAC-ID in a separate database.

3. Once an identity is created, the BlackRidge Cloud Gateway responds to the TAC-ID with an acceptance message and a unique "token" hash created for the identity. When the TAC-ID receives this hash, it begins sending "tokenized" traffic to the BlackRidge Cloud Gateway by attaching this hash directly to outgoing packets.

4. Upon receiving tokenized traffic with the proper hash, the BlackRidge Cloud Gateway allows traffic from the TAC-ID to reach the FTP server. Since all authentication exchanges happen between the TAC-ID and AWS Gateway, the process is 100% transparent to both the IoT device and the FTP server.

5. To save bandwidth, the BlackRidge Cloud Gateway only requires a hash from the TAC-ID for the first packet sent in the connection. All subsequent traffic in the session does not require the hash, which prevents connection lag between the IoT device and the FTP server.

About BlackRidge Technology

BlackRidge Technology enables our customers and partners to deliver more secure and resilient business services in today's rapidly evolving cyber threat environments. The BlackRidge adaptive cyber defense solution authenticates identity before allowing network connections to proactively isolate cloud services, protect servers and IoT devices, and segment networks**.** Our patented technology authenticates user or device identity and enforces security policy on the first packet of network sessions. This new level of real-time protection blocks or redirects unidentified and unauthorized traffic to stop port scanning, cyber-attacks and unauthorized access. BlackRidge was founded in 2010 to commercialize its military grade and patented network security technologies.