CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY — CISA

EC3 — Emergency Communications Cybersecurity Center

REDUCE ECC CYBER INCIDENTS THROUGH SEGMENTATION*

When federal, state, local, tribal, and territorial information technology (IT) systems are affected by malware, it may traverse the local IT network and infect critical systems within the Emergency Communications Center (ECC). One technique to strengthen security is network segmentation.

Network segmentation is a physical or virtual architecture approach dividing a network into separate segments. Each segment acts as its own independent subnet, creating a boundary between networks and providing additional security and control. Network segmentation also limits access to devices, data, and applications, restricting communications between the IT network and the ECC. This prevents malicious actors from gaining access to critical systems within the ECC.

Firewalls and components (such as a switch) acting as a Demilitarized Zone (DMZ) are used to create the segmentation. Firewalls can be configured to block traffic from network addresses, applications, or ports, while allowing necessary data through. In addition to firewalls, policies and controls should be used to monitor and regulate system access and traffic between network segments.

*See CISA's companion document, "Layering Network Security Through Segmentation" infographic.

Figure 1: Unsegmented IT/Municipal Network

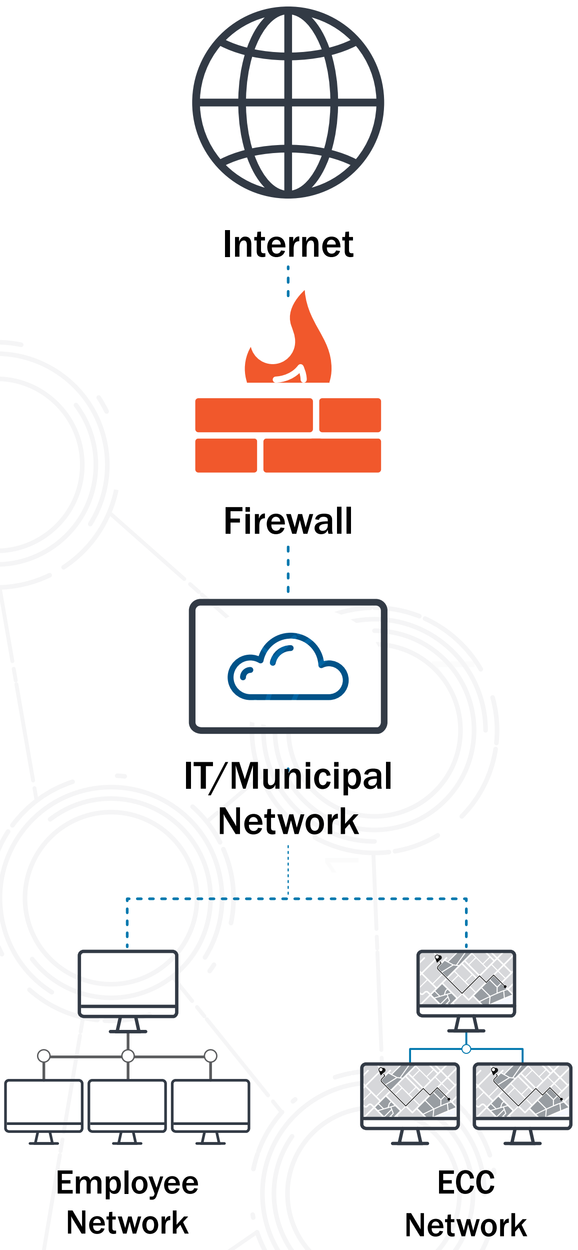
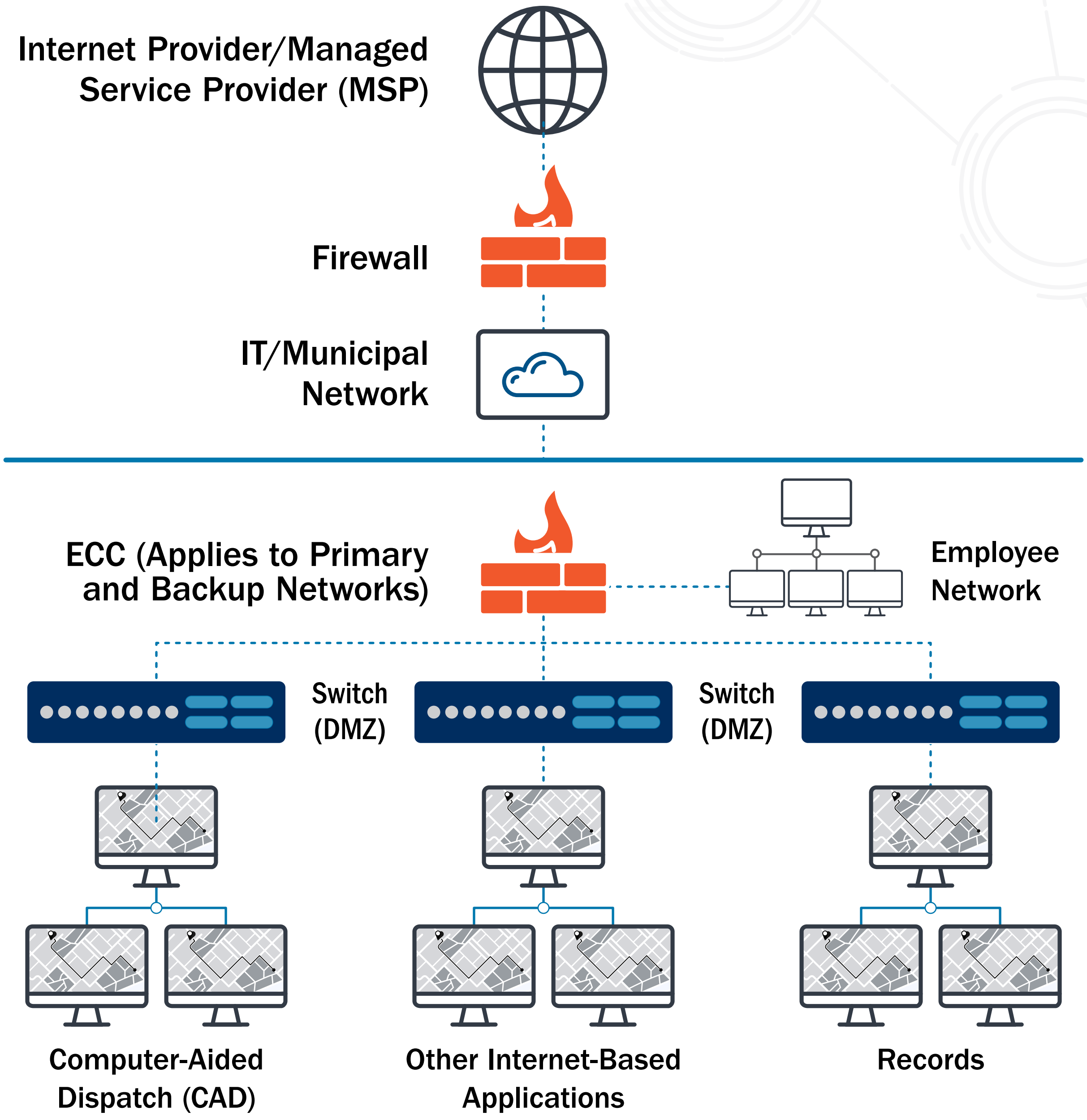


Figure 2: ECC Critical Systems Segmented from IT/Municipal Network


Internet Provider/Managed Service Provider (MSP)
Firewall
IT/Municipal Network
ECC (Applies to Primary and Backup Networks)
Employee Network
Switch (DMZ)
Switch (DMZ)
Computer-Aided Dispatch (CAD)
Other Internet-Based Applications
Records

Unsegmented Risks

Attacks affecting the municipal network, such as malware, can enter the ECC and impact critical applications such as CAD.

Segmenting Benefits

- The ECC is isolated from the municipal network and is not impacted by attacks such as malware
- Grouping CAD workstations into segments allows for continuity of operations in the event one segment becomes infected with malware
- Any system (e.g., workstation, application) requiring internet access can benefit from network segmentation

Recommendations

- Establish a segmented high security zone for the ECC
- Protect access to devices within this zone by using specific firewall access controls
- Separate CAD workstations into groups and establish a segmented zone for each group
- Limit data traffic to the ECC network with remote access control

cisa.gov | EC3@hq.dhs.gov | Linkedin.com/company/cisagov | @cisagov | @cyber | @uscert gov | Facebook.com/CISA | @cisagov