SECURING BACK-END COMMUNICATIONS BETWEEN MUNICIPAL ENTITIES IN A REGIONAL DISPATCH OPERATIONS:

Keeping Billy Bob out of your Network while Maintaining Access to Critical Information Resources

By

Mike Weiss

To

Dr. RAY KLUMP

(INFORMATION SECURITY PRACTICUM)

68-595K-SP12

MASTER OF SCIENCE
In
INFORMATION SECURITY

LEWIS UNIVERSITY

April 2012

ABSTRACT

The financial challenges faced by municipalities today have forced them to look at avenues to reduce costs even in critical emergency response divisions. These challenges have led to the formation of Regional Dispatch Centers that seek to save costs by consolidating dispatch operations while serving multiple municipal areas. Staff and equipment can be de-duplicated in this process however, it opens up new challenges for security and data delivery between the municipalities. This paper seeks to lay out a foundation for connecting municipal entities through a dedicated network in order to offer data delivery services while still maintaining the security of the host site as well as the municipal entities that participate in the Regional Dispatch operation. The consolidation of efforts in utilizing the dedicated network model can be a challenging proposition because the municipal entities enticed by this de-duplication are generally cash-strapped and rarely even have dedicated IT Departments. The hope is that standardized equipment kits and simplified deployment can maintain strong defensive measures while also allowing the municipalities to participate in the Regional Dispatch operation without significant risk or cost. This paper lays out the equipment and configuration required for the host site, the entity responsible for the network's operation, as well as the options available to subscribe to the participating municipal entities.

Table of Contents

1. INTRODUCTION

With the increased budget constraints that have come with the "Great Recession [1]", municipal entities have to contend with much lower revenues while continuing to provide critical services for the public, such as Police, Fire, and Emergency 9-1-1 service. One way municipal entities are addressing the loss of revenue is by regionalizing services to share costs and de-duplicate some of the infrastructure, including buildings, staff and equipment [2].

A growing trend, and one that gets additional attention from grant boards, is setting up Regional Dispatch Centers where a single dispatch operation serves multiple communities or even entire counties. These regional dispatch centers generally function under the direction of one municipality, known as the "host", entity and receive funds from other municipal entities, also referred to as "subscribers", to provide Police, Fire and Medical Dispatching services. As is common with most services today, the dispatchers utilize Computer-Aided-Dispatch (CAD) software to facilitate efficient collection of information and accurate personnel direction to include apparatus selection when dispatching units are on a call. Although the CAD software is generally served at the host's site, the member municipalities must have the data integrated into their own Records Management Systems (RMS) to facilitate the Police and Fire officers' access to data for their reports and records retention. Examples of this include the Southwest Regional Communications Center [3], the Northern Ellis Emergency Dispatch (NEED) Center [4], and the Washington County Dispatch Center.

Integration is setup through a back channel connection, such as Fiber or Point-to-Point Microwave, which connects the entities together at a point, generally deep within their network. The challenge for municipal IT Departments is maintaining system integrity and security while still providing access to agencies that they have no control over, both from a management and technological standpoint. The point of regionalization is to assist smaller entities that do not have the funding or budgets to support the needs of the dispatch operations. This is a double-edged sword because these same entities also do not have the resources to support even an IT Department and so contractors are used even though they often may not have the necessary experience or training to adequately support the challenges associated with municipal entities. For instance, most contractors do not have the State certification required to work on dispatch computers or even, technically, be in the same room as them [5].

The challenge for the host site is to design a secure and stable network that can provide the resources that the subscribers require to be able to do their jobs and meet the Federal, State, and Local records and information retention requirements while keeping curious or untrained staff at those subscribers from damaging or accessing information within the host's network.

CJIS's Role in the Network

The Criminal Justice Information Services (CJIS) is a Division within the Federal Bureau of Investigation (FBI) that manages the information resources that have been made available through agreements with State and Local agencies in order to provide "timely and secure access to services that provide data wherever and whenever for stopping and reducing crime" [5]. In order to protect this data, each agency that wishes to access this data must adhere to the security policy created to protect that information, commonly known as the *CJIS Security Policy* [5]. This policy is based on National Institute of Standards and Technology principles and is periodically updated to reflect changes in technology and business models.

In 2011, the FBI authorized a major update to the *CJIS Security Policy* regarding access to major criminal history databases that local Police agencies rely on when verifying a person's criminal and driving background. This policy, in turn, was adopted by the State of Texas, which acts as an intermediary for access to the FBI databases in the State of Texas, as a requirement for compliance from all local Police agencies [6]. Each agency has a periodic review of their systems to ensure compliance with the current *CJIS Security Policy*. If an agency is non-compliant, then it is possible their access to these resources could be revoked making enforcement and detection of possible criminals difficult. Any system put in place that transmits protected CJIS data has to meet these requirements and so the *CJIS Security Policy* creates a focal point to not only maintain compliance for access to FBI resources but also provides a good resource for recommended principles for securing networks against intrusion to maintain the integrity and confidentiality of data.

Within the security policy, it is necessary to "ensure any connections to the Internet, other external networks, or information systems occur through controlled interfaces (e.g. proxies, gateways, routers, firewalls, encrypted tunnels)." [5] The errata on this section of the policy is taken that it is a requirement to place a firewall between Police agencies when connecting their networks together, since they are not a part of the same agency or municipal entity. Though to an outsider these may seem like a part of the same system (e.g. the government), they are legally separate entities and thus any connection to another agency constitutes an external connection. This requirement throws out a common practice among agencies: connecting their networks directly via T1, Fiber or microwave communications.

Plotting a Path

This paper will look at the overall design of an Emergency Network which will provide direct communications between any number of municipal entities. The network will be setup in such a way to allow any number of additional entities to subscribe, participate and fully integrate into the network. Once an overall network design is delineated, the hardware required for this integration, such as the firewall’s, router’s, and other devices. will be discussed in detail. This includes looking at the hardware itself and the settings and overall policy which will facilitate secure communications and secure equipment to minimize as much risk to the network as possible while maintaining a conscious eye on costs and administrative overhead. Finally, a review of the *CJIS Security Policy* and the requirements on municipal entities participating in this network will be discussed with the goal being to make sure this network maintains compliance.

2. DESIGNING THE NETWORK

In order for the Regional Dispatch model to function efficiently each municipality will have to connect their Policy systems together to create a network. This will be referred to as the Emergency Network and is, essentially, a set of back-end connections to other municipal Police Department agencies used to facilitate the transfer of information from the CAD systems at the host site to the RMS systems at the subscriber sites. This communication is not always one direction and it is possible that subscriber agencies will need to pass information up to the host site so this must be taken into consideration in the design and implementation of the network.

Because each municipality is a separate legal entity and have different IT policies, education, training and staff knowledge, each entity must treat the connection to the Emergency Network as if it were an external connection, such as a connection to the Internet, and should protect it accordingly. Looking from above, the network begins to take shape as seen in Figure 1.

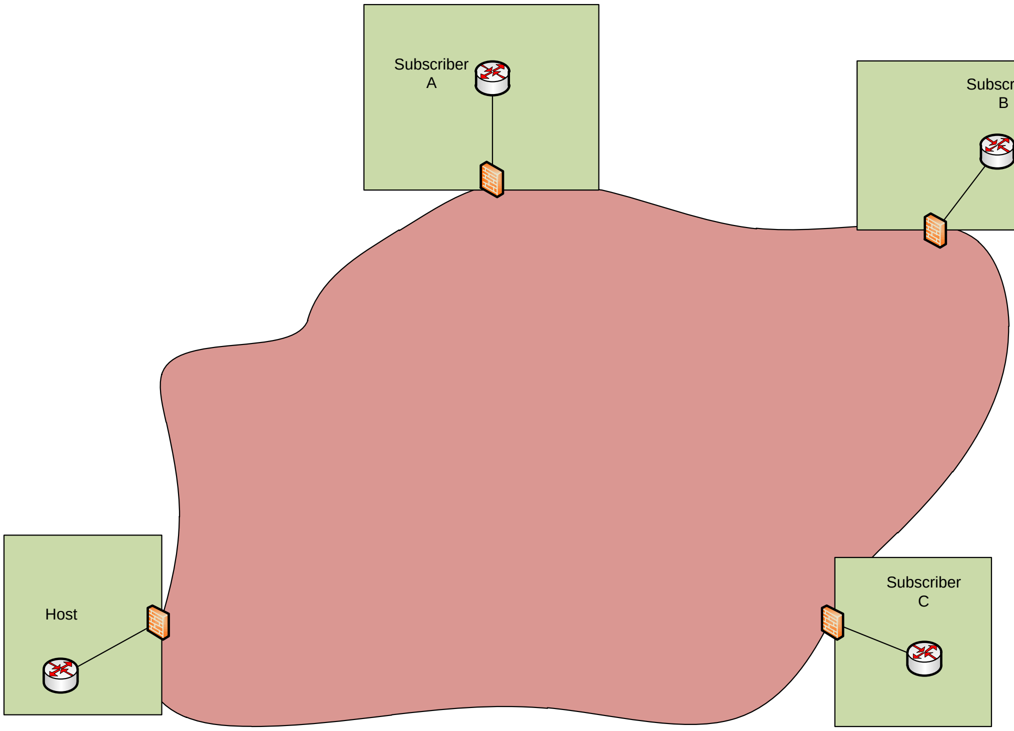


Figure 1: Network Concept A

Essentially, the host and all of the subscriber agencies will connect to the regional network. However, each agency will treat everything outside the network as hostile. Specific traffic will be allowed through the firewalls at each site. The challenge is getting the network to communicate in a way that maintains the security of the data, ensures access is maintained even with failure of some parts and allows for high-speed communication between agencies.

Structure, Design, and Authority

In the interlocal agreement that sets up the Regional Dispatch Operation, the host site is given authority to design and setup the network, administer the policies for access and security of the Emergency Network and designate the authorized devices and traffic allowed on the network.

With the possibility that some subscriber sites will lack an IT Department and have varying degrees of skill and knowledge at each site a goal of the project is to setup a standard hardware package, called a ‘hook kit’ that can be deployed at each agency as it comes onboard with the Regional Dispatch Center. These standard packages of equipment are almost identical for each agency and are designed to easily hook into an agency’s existing network and provide a redundant and secure connection back to the host’s servers.

The design of the network uses the small inexpensive Cisco ASA 5505 firewalls to secure each site using Network Address Translation (NAT) [7] to hide the host and entity networks while classifying any unknown outside traffic as hostile. Ensuring the firewalls are correctly setup and properly configured to allow necessary traffic while stopping any extraneous traffic is key in defending the host and subscriber sites. Since this network is used to enable communications from the host dispatch center and the subscriber agencies, it is important for the host agency to set guidelines on the appropriate traffic and utilize the firewalls to provide technical controls and limitations on that traffic. Additionally, Cisco routers are used to enable

Enhanced Interior Gateway Routing Protocol (EIGRP) [8] at each site to establish a redundant network using point-to-point microwave links to form a mini-web. Microwave communications provide a stable, reliable and economical solution to connecting agencies that can reside in excess of 15 miles from each other.

Another way to separate the agencies and provide a mechanism for securing the sites is by subnetting the Emergency Network and removing them from the access layer of the network [9]. This provides a way to increase the security options on the network in future deployments. Inserting a router outside of the firewall also provides a way to utilize distance-vector routing protocols [10] allowing the use of redundant links to maintain network connectivity in the event that one of the links goes down. The final design is able to maintain connection through multiple failures in certain situations. Returning to the network design overview the network takes more shape, as can be seen in Figure 2.

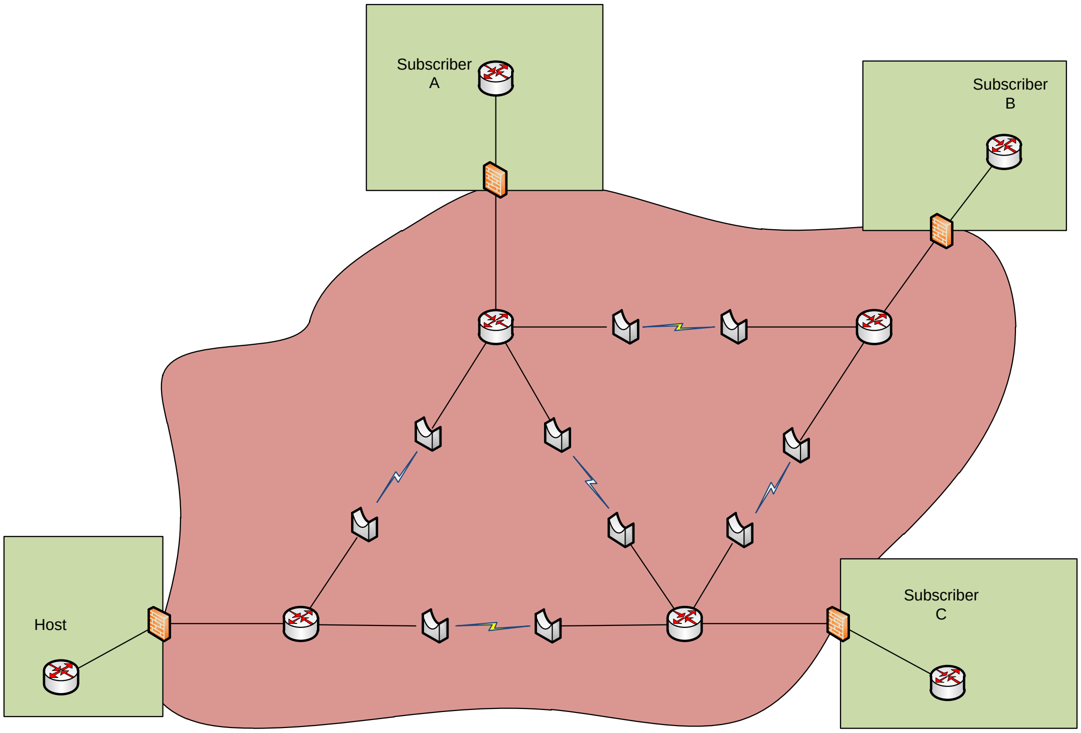


Figure 2: Network Concept B

The components of the project are designed to be dynamic and flexible. This model allows additional sites to be integrated into the Emergency Network with little or no technical knowledge, which ensures that even sites without an IT department or onsite technical staff can integrate. These 'hook kits' also provide a standardized equipment list so each agency has a clear cost of integration. The hook kit's standardized nature also helps eliminate misconfigurations at each site making it easier to protect properly each agency from each other without needing a Master's degree in Information Security.

3. SECURING THE HARDWARE

The distributed nature of the Emergency Network means that devices will be placed in locations that are accessible by staff outside of the authority and control of the host site, an issue that is at the core of the security problem for this project. Though these devices reside in secure sections of the subscriber sites from a CJIS perspective, which is defined as "a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJIS and associated information systems. [5]" This space is not secure from the perspective of the host site. As such, it is important to pay attention to not only the hardening best practices [11] but also additional settings and controls that can aid in maintaining the integrity of the data on the network and the availability of the network itself. The routers and microwave links themselves need to be properly secured and hardened because they reside in physical locations to which all subscribers have access.

Router Setup

Though the routers reside at each site, and they are provided by the site to which they reside, their function is critical to the efficient operation of the overall Emergency Network. As such, access to the devices will be limited to personnel from the host site. The routers are preconfigured with the settings necessary to attach to the network by the host site.

Cisco C880 routers are used for this application. They are small, inexpensive, and are powerful units with the ability (when purchased with IP Services software license) to perform dynamic routing, which is important to easily update the network routes as additional sites come online. Without a dynamic routing protocol enabled, each time a new site is added all of the routers would need to be updated with the new route destinations. The dynamic routing will also allow redundant routes on the network and will prevent these links from becoming routing loops [8].

The routers need to be hardened, including setting up a user account and utilizing the `secret` command to take advantage of a stronger encryption algorithm than what is provided in the old `password` command [11]. Using the secret command encrypts the passwords with a MD5 hash and can be achieved using the command:

```
!
username <name> secret <secret>
!
```

Setting an `enable` password is also effective at partitioning user accounts from administrative access to the system and provides an additional layer of protection for the device. Also, setting the `no service password-recovery` option prevents an attacker with console access to the device from insecurely accessing the device configuration or clearing the passwords. This options is set simply using the command:

```
!
no service password-recovery
!
```

A local username and password should always be used in case the remote authentication mechanism, if used, is offline or unavailable. The router will fall back to the local user database to grant access.

There are a couple of options for dealing with users for the routers at this point each with their own caveats and options. It is possible to simply utilize the local user database on the routers to grant access to the device or Authentication, Authorization, and Accounting (AAA) can be setup to authenticate and authorize access to the routers. Using the local user database is simpler to setup, does not require additional access to the host site servers for authorization and is not vulnerable to dictionary attacks against network traffic containing the shared secret [12].

If the shared secret of the device is compromised, it would give the attacker access to all passwords and information sent from the router to the RADIUS host. This vulnerability has the potential for being incredibly damaging. If an administrator account is used to login to the router from the host network this would give the attacker administrator access in the host network. At that point it's game over for the host network.

However, utilizing AAA provides additional reporting and auditing capabilities, which could provide additional information in detecting a possible intrusion or attack attempt on the Emergency Network. This would require that the host site have a RADIUS server setup and is accessible from the Emergency Network. A limitation of the Cisco routers is they must use Password Authentication Protocol (PAP) when communicating with Microsoft IAS. This model "uses plaintext passwords and is the least secure authentication protocol" [13]. Security can be heightened by utilizing Cisco's TACACS+ but this would require additional, significant investment at the host site.

It is a good practice to disable any communication services that do not utilize encryption (such as Telnet). Using Secure Shell (SSH) instead is far more desirable as passwords and commands are not sent in clear text across the network [14]. Even if the encrypted tunnel is compromised the damage to the system is minimal because the damage would be limited to the single router. In either case, using some encryption when communicating over the less secure sections of the Emergency Network is preferable to using protocols, such as Telnet, that do not use any encryption and transmit all data in plaintext. Secure Shell can be enforced on the router by restricting connections to allow only SSH. The example below generates a crypto key for use in creating the SSH tunnels, sets a login failure maximum before disconnection, sets a timeout for idle sessions and allows only SSH connections to the router:

```
!
ip domain-name example.com
!
crypto key generate rsa modulus 2048
!
ip ssh time-out 60
ip ssh authentication-retries 3
!
line vty 0 4
transport input ssh
!
```

Since these devices sit outside the host site's network, it is possible that an attacker could access a less secure subscriber and sniff traffic. Limiting the amount of unencrypted traffic is essential in this case especially when potentially transmitting passwords to the routers.

Additional physical security precautions should be taken to limit an attacker's access to the routers. This includes disabling the console port and any unused ports on the router. Ideally, the router and microwave radio equipment should be locked in a network enclosure that also protects the power or network connections from being disconnected. However, this is a limited security measure because the network connections ultimately must connect with a subscriber's network and that point on becomes vulnerable to potential security practices that are less than ideal.

In order to enable alternate routing each link from the router needs to be on a different subnet. The host and subscriber sites will also each be located on its own subnet to allow access from multiple links. In this case, it is known that there will be four devices between each site: router A's interface, router B's interface and two microwave bridges as seen on Figure 3. Thus, a subnet mask of 255.255.255.248 (CIDR /29) is used with six available addresses.

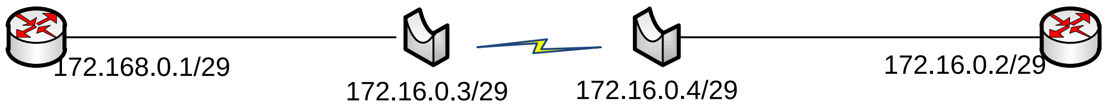


Figure 3: Link Detail

Each site is assigned a unique subnet of its own, allowing any other site to access it using the same ip address. For instance, if the host site is given the subnet 172.16.11.0/24 and assigns a 'public' address of 172.16.11.11 for one of the servers all of the subscriber sites would be able to use the same ip address to reach that server even if they are accessing it from different subnets or links on the routers. Though this subnet can be scaled the same as the router links, it is always a good idea to leave enough addresses for future needs. For this network, the 172.16.0.0 private network is being used giving plenty of assignable addresses. Each site is given a 24-bit subnet mask allowing the use of up to 254 addresses. The .1 address is reserved for the router interface and serves as the gateway address for the subnet. The .5 address is reserved for each of the site firewalls. The remaining addresses in the range below .11 are reserved for future router or firewall interfaces allowing the sites to assign addresses at .11 and above.

With each site assigned a subnet, traffic can be filtered and easily identified in the event of an attack. An entire site can be isolated or banned if malicious or questionable data is received from the site. Network segmentation also increases network performance by reducing network congestion and reducing the size of the broadcast domain [15]. It is also possible, if desired, to hide the subscriber sites from each other entirely. This can be achieved by setting up Access Control Lists (ACLs). In some cases, this is helpful if the subscriber sites do not want to receive data from other subscribers, though it is not necessary. Since the host site, and not the subscribers manage the routers, it makes it more difficult to change settings on the fly if two subscriber sites want to share data, as they have to involve the host site to make adjustments in the router's ACLs. Because of this, it makes more sense to utilize the firewalls, which the subscriber sites control, as a point of control when dealing with subscriber-to-subscriber communications.

Firewall Setup

At the border of each site's network, it is imperative to place a firewall for a number of reasons. The firewall creates a powerful security guard allowing granular control over the data that is allowed into the site's network. It also provides several needed network services, such as anomaly detection, stateful inspection and Network Address Translation (NAT) [16]. Cisco ASA 5505 firewalls are selected because they are able to handle all of the necessary functions: they are capable of EIGRP, they have an easy to use GUI and they are incredible stable and affordable firewalls [7].

The limited nature of the Emergency Network makes the firewall setup easy because there are only a few services that the host site needs to allow access. The subscriber sites access the host site's CAD Server database and pull the incident information related to their site. The CAD software manages the security divisions between incidents (ensuring that subscribers retrieve only data pertaining to their agency).

NAT is used on both ends of the connection between sites. On the host site, it is used to mask the internal IP address of the CAD Server; and on the subscriber side, it is used to mask the internal IP address of the RMS. Using the NAT information, the firewalls can be setup to permit only traffic from the NAT address of the RMS Servers at the subscriber sites to the NAT address of the host site's CAD Server. This can further be locked down to allow only traffic on the port that the database answers on. By default, this would be port 1433 [17], since the backend database is running on SQL Server. However, it is advisable that this port be changed to a different port to obscure the traffic. Using this technique, only the named RMS Servers will be able to communicate through the host firewall making it far more difficult for someone outside the host network to access that server inappropriately. This technique also thwarts almost all script-kiddie SQL-injection tools that have been preconfigured to look for SQL databases answering on port 1433.

With the firewalls simply sitting between the Emergency Network and the host’s, or subscribers, internal networks there are really only two interfaces that need to be defined at each site: the internal and external. All of the other interfaces can be disabled. The internal interface will connect with the host or subscriber’s network and the outside interface will connect with the Emergency Network. This keeps in line with our principle of treating the Emergency Network as hostile and, by default, the Cisco Firewalls will not trust any traffic coming into the outside interface unless explicitly instructed. A Virtual Local Area Network (VLAN) is used to achieve this division and allows assignment of a security level at each interface. Assigning different security levels lets the firewall treat incoming and outgoing traffic from those interfaces differently and determines whether additional screening needs to be done on the traffic. By default, the ASA firewalls arrive preconfigured with two VLAN’s: outside and inside with appropriate security levels so this does not need to be changed [18]. Each interface will need to be set with the internal and external IP address, which will both be unique for each site. The internal address is the address to which all traffic destined for the Emergency Network needs to be directed as the gateway address. This is imperative to set on the internal network at both the host and subscriber sites. The host site interfaces would look something like:

```
interface Vlan1
```

```
 nameif inside
 security-level 100
 ip address 192.168.10.11 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 172.16.11.5 255.255.255.0
!
```

Additionally, each site will need to have NAT configured to translate the internal addresses that need to be accessed from the emergency network. The host site will need to NAT the servers that will be hosting services, most notably the CAD servers, which need to communicate with the subscriber's RMS Servers. This can be done either by first defining named objects and then assigning NAT to the named objects or by simply defining the NAT rule based on the IP address of the server. Ideally, named objects would be used to make it easier to see which server is being setup with NAT. This can be utilized later when setting firewall rules as well. Below are examples of the NAT rule setup both using named objects and simply using the IP address of the server:

```
static (inside,outside) Cad-Server_Public Cad-Server netmask 255.255.255.255
static (inside,outside) 172.16.11.250 192.168.14.41 netmask 255.255.255.255
```

The example above represents a static NAT access control list (ACL) and defines a host on the inside network with an outside IP Address. The first name, or IP address, is the Emergency Network IP address (and the one used by the subscribers to connect to the server), while the second name, or IP address, is the inside network of the server. Finally, the netmask is defined which is a 32-bit mask to identify a single host. The netmask must be defined on the host network's firewall to allow services to function. Moreover, NAT will also be applied on the subscriber firewalls to separate traffic from authorized servers. This configuration allows for later enhancement of the firewall access-list rules to permit any traffic from authorized servers on specific ports and gives very granular control over the communications that are allowed through the host firewall.

In order to allow actual network traffic to pass across the firewall, rules must be defined to permit the traffic [19]. These rules are applied to the outside interface access-list and must define the source, destination and service or ports that will be allowed. As the host network or the subscriber-to-subscriber adds additional services, the access-list tables are modified to permit traffic to additional services if necessary. The access-list below is an example of the tables that need to be defined:

```
access-list outside_access_in extended permit object-group CAD any host Cad-Server_Public

access-list outside_access_in extended permit object-group CAD object-group CAD_authorized host Cad-Server_Public
```

As can be seen in the example above, the first access-list allows any host to access the CAD Server's public ip address on any port defined in the CAD group. This is not an ideal access-list because the scope of allowed hosts is too broad. Instead, the second rule is more desirable. This rule allows any host defined in the "CAD_authorized" group to access the CAD Server's public IP address on any port defined in the CAD group. The object-groups that would need to accompany this rule include a list for the allowed ports and a list of authorized computers for accessing the CAD server. The CAD_authorized group would look like:

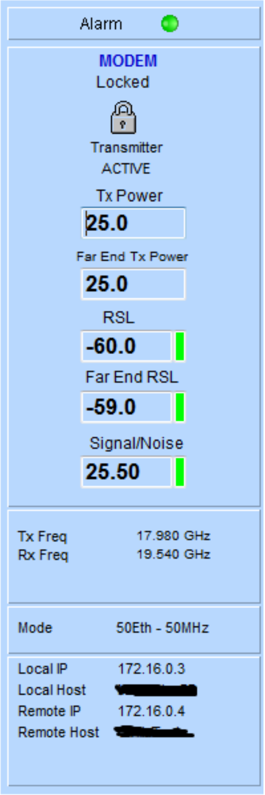
```
object-group network CAD_authorized
 network-object host 172.16.12.11
 network-object host 172.16.13.11
```

```
object-group network RMS_authorized
 network-object host 172.16.12.11
 network-object host 172.16.13.11
```

There are two object-groups defined above: CAD_authorized and RMS_authorized. Each group contains the same two hosts (172.16.12.11 and 172.16.13.11) and simply makes it easy to reference the two hosts when creating rules. For instance, without the group each host would have to be given access to the CAD server's public IP address individually making it necessary to create two separate rules. However, by defining the object-group with the two hosts included a single rule can be created. This is a more efficient way of creating access-lists but care should be taken so that hosts that should not have access to a resource are accidentally given access because they are included in a group.

Wireless Bridge Setup

The wireless bridges used for the project are Cielo Networks high-powered microwaves. The units are easy to setup and configure, are capable of encrypting all traffic using 256-bit AES and include an easy to read console checking on any issues, as seen on Figure 4. Also, these units are able to send SNMP traps to a trap server for correlating logs [20].



Alarm ●

MODEM
Locked

Transmitter
ACTIVE

Tx Power
25.0

Far End Tx Power
25.0

RSL
-60.0 🟩

Far End RSL
-59.0 🟩

Signal/Noise
25.50 🟩

Tx Freq 17.980 GHz
Rx Freq 19.540 GHz

Mode 50Eth - 50MHz

Local IP 172.16.0.3
Local Host [redacted]
Remote IP 172.16.0.4
Remote Host [redacted]

Figure 4: Microwave Status Console

The most important details on the microwave setup is to be sure and change the default administrator passwords as this is typically overlooked. Also, depending on the type of microwave used, it is possible that a FCC license is required for operating units that don’t function in the public bands. This is an important decision point for the project as a microwave that functions on the public bands (900Mhz, 2.4GHz, 5.3GHz, 5.4GHz or 5.8GHz) [21]don’t need a FCC license but can have problems with other microwave units in the area.

Using a licensed band microwave (which operates in the 6Ghz, 11GHz, 18GHz, 20GHz or the 80GHz) [21] requires a license from the FCC and that can be a time-consuming and costly process. However, once licensed it is highly improbable that there will be any interference from other microwave units in the area. For this project, entities will be able to use a third classification: public safety bands. These units operate in the 4.9GHz band and do not require a license per se but do require the local users to coordinate with each other. This band is dedicated to public safety purposes such and police, fire or video backhaul.

4. CJIS SECURITY POLICY REVIEW

The *CJIS Security Policy* is a fairly long and broad document dealing mostly with policies that fall primarily under the jurisdiction of the Police Department such as staff training, Officer responsibilities, appropriate use of the data and controlling access to the terminals that can view any data from the CJIS databases. There are also areas that are important for IT to be aware of but which are outside the scope of the Emergency Network design such as use of Bluetooth devices, laptop security requirements, user identification and VOIP (Voice over IP) protocol controls. However, there are key areas of the network that will be tested by the *CJIS Security Policy*. As with most policies, there is room for interpretation as differences in technology and setups are common. This allows each agency some room for flexibility but also can become a problem if there is a disagreement on the implementation of one of the requirements.

Several areas of note are the firewall protections for each agency, the wireless communications utilized, the physical protections for the network equipment and guarding against unauthorized access to the network. Rule 5.10.1: Information Flow Enforcement is an important area to be aware of. This rule requires that all information that flows between interconnected systems do so in a controlled manner that keeps the CJI (Criminal Justice Information) secure while in transit across the system [5]. Also, this rule requires that the agency "monitor and control communications at the external boundary of the information system and at key internal boundaries within the system. [5]" This is where the importance of using a good, feature-rich, firewall is important. Although the basic requirement is to secure these external boundaries, such as those linking other municipalities to each other, there is a further requirement to monitor those connections to "monitor network connections, detect attacks, and provide identification of unauthorized use" [5] which is a feature of the Cisco 5505 [7].

The network design is sufficiently secure and meets the policy requirements. Each site is protected by a firewall to the ‘outside’ Emergency Network and is thus protected from each other by a FIPS140-2 compliant firewall [22] as required by rule 5.10.1.1 [5]. The traffic into the network is authorized (by segregating the NAT of the servers from the dynamic NAT pool of the firewall); the firewall logs and monitors for any possible attacks or possible unauthorized access to the network.

On the wireless link side, the point-to-point microwave connections are setup with 256-bit AES encryption and, again, is in accordance with the FIPS-140-2 requirements on rule 5.10.1.2. Network equipment is stored in a secure section of the host and subscriber agency’s building, as defined in the *CJIS Security Policy* under section 5.9.1 [5], and is locked even beyond access by the officers at each subscriber site.

It is also important to maintain a current and detailed network map of the interconnected municipalities. During an audit, the auditors will utilize that map to review key areas of the network and it will be instrumental in determining compliance with the policy. Further, it is incredibly important to label this map with “For Official Use Only” [5]. Without this designation, who knows in what way a curious by-stander may use this critical document! Many an agency has been deemed out of compliance for not correctly labeling their critical documents.

5. BRINGING IT ALL TOGETHER

The host site maintains a least privilege posture to any communications entering the site and all extraneous network traffic is dropped by the host firewall. The Emergency Network is able to provide communications that are necessary for the regional dispatch center to function but keeps the host site secure from intrusion or unauthorized access from the potentially less secure subscriber sites. The key is in treating the other agency networks the same way that the network is treated: as potentially hostile. This guides the controls and configurations in such a way that protects the host site while continuing to provide access to the resources that the subscriber sites need to continue functioning efficiently.

The main components of the hook kit: firewall, router, microwave bridges which can be pre-staged by the host site with the majority of the settings necessary to bring a new subscriber site online with very little interaction. The two main setups that the subscriber sites need to provide are the internal IP address for the firewall and to configure a route on their network to direct traffic destined for the Emergency Network. The host site should provide documentation for adding additional firewall rules to the subscriber sites so that they can adjust their settings as needed in the event that they host services for other sites. The subscriber sites, however, only need minor involvement to connect to the Emergency Network. Even with limited resources and potential security breaches at the subscriber sites, the host site is able to maintain a strong security perimeter against unwanted intrusion or attacks.

In the future, the network strength should be tested either using an outside consulting company or by utilizing some of the many tools available such as Nessus [23], Metasploit [24] or GFI LanGuard [25]. This can be a long and time-consuming process but it can highlight weak areas of the network and provide a way to further strengthen the network while also providing confirmation that the techniques currently used to secure the network are effective. The results of a penetration test will also provide insight into additional security safeguards that would be helpful to implement in the future.

Though this particular setup is specific to municipal government, and there are a number of regulations and protocols that are specific to that industry, this model can be used for any system requiring a backend connection between multiple entities. Similar setups can be used to link regional hospitals that are a part of the same system, schools or even businesses. Most of these bodies generally choose to use VPN tunnels over the internet, which is a perfectly good way to do it. However, this model sets up a more stable and secure connection which can be beneficial when security is paramount.

BIBIOGRAPHY

[1] D. Wessel, "Did 'Great Recession' Live Up to the Name?," *Wall Street Journal,* 2010.

[2] J. Wenzel, "Town Council Considers Regional Dispatch Center," 22 11 2011. [Online]. Available: http://rockyhill.patch.com/articles/town-council-considers-regional-dispatch-center.

[3] Southwest Regional Communications Center, "Southwest Regional Communications Center," [Online]. Available: http://www.swrcc.net/pages/about.php.

[4] City of Midlothian , "Northern Ellis Emergency Dispatch," [Online]. Available: http://www.midlothian.tx.us/index.aspx?NID=163.

[5] Federal Bureau of Investigation, "Criminal Justice Information Services (CJIS) Security Policy," 2011. [Online]. Available: http://www.txdps.state.tx.us/SecurityReview/CJISSecurityPolicyv5.pdf.

[6] Texas DPS, "Requirement and Transition Document," [Online]. Available: http://www.txdps.state.tx.us/SecurityReview/reqTransition.pdf.

[7] Cisco Systems, "Cisco ASA 5500 Series Adaptive Security Appliances," [Online]. Available: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html.

[8] R. Malhotra, "Chaper 4 - Enhanced Interior Gateway Routing Protocol (EIGRP)," 2001. [Online]. Available: http://oreilly.com/catalog/iprouting/chapter/ch04.html.

[9] Netscreen Technologies, "Principles of Secure Network Design," 2001. [Online]. Available: http://www.packetnexus.com/docs/CASE_260_002_Principles_of_Secure_Network_Design_v1_1.pdf.

[10] G. Malkin, "RIP Version 2," 1998. [Online]. Available: http://www.ietf.org/rfc/rfc2453.txt.

[11] Cisco Systems, "Cisco Guide to Harden Cisco IOS Devices," 07 06 2011. [Online]. Available: http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080120f48.shtml.

[12] B. Aboba, "RADIUS Security Issues," 29 6 2005. [Online]. Available: http://www.drizzle.com/~aboba/RADEXT/NIST-RADIUS.ppt.

[13] Microsoft, "Password-Based Authentication Methods," [Online]. Available: http://technet.microsoft.com/en-us/library/cc732393%28v=ws.10%29.aspx.

[14] Cisco Systems, "Configuring Secure Shell on Routers and Switches Running Cisco IOS," 28 06 2007. [Online]. Available: http://www.cisco.com/en/US/tech/tk583/tk617/technologies_tech_note09186a00800949e2.shtml.

[15] DISC, "Defense in Depth and Network Segmentation," 10 02 2009. [Online]. Available: http://blog.deurainfosec.com/defense-in-depth-and-network-segmentation.

[16] Cisco Systems, "How NAT Works," 29 03 2011. [Online]. Available: http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094831.shtml.

[17] Microsoft , "TCP/IP Port Numbers Required to Communicate to SQL over a Firewall," [Online]. Available: http://support.microsoft.com/kb/287932.

[18] Cisco, "Cisco ASA Getting Started Guide, Version 7.2," [Online]. Available: http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/start.html#wp1054582.

[19] Cisco, "Configuring IP Access Lists," [Online]. Available: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00800a5b9a.shtml.

[20] Network Working Group, "A Simple Network Management Protocol (SNMP)," [Online]. Available: http://www.ietf.org/rfc/rfc1157.txt.

[21] J. Wargo, "Alpha Omega Wireless Blog," 27 06 2010. [Online]. Available: http://www.aowireless.com/blog/bid/42478/Understanding-Microwave-Communication-Frequencies.

[22] Cisco, "FIPS 140-2 Non-Proprietary Security Policy for the Cisco ASA 5500 Series Security Appliance," [Online]. Available: http://www.cisco.com/en/US/docs/security/asa/asa70/hw/fips_asa.html.

[23] Tenable Security, "Tenable Network Security," [Online]. Available: http://www.tenable.com/products/nessus.

[24] Rapid7, "Metasploit," [Online]. Available: http://www.metasploit.com/.

[25] GFI Software, "GFI Languard," [Online]. Available: http://www.gfi.com/network-security-vulnerability-scanner.

[26] Cisco Systems, "Introduction to Firewall Services," Cisco, [Online]. Available: http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/4.0/user/guide/porules.html.

[27] Cisco Systems, "Introduction to EIGRP," Cisco, 10 08 2005. [Online]. Available: http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080093f07.shtml.

[28] National Security Agency, "Defense in Depth," 2011. [Online]. Available: http://www.nsa.gov/ia/_files/support/defenseindepth.pdf.

[29] J. Wenzel, "Town Council Considers Regional Dispatch Center," 22 11 2011. [Online]. Available: http://rockyhill.patch.com/articles/town-council-considers-regional-dispatch-center.

[30] Southwest Regional Communications Center, "Southwest Regional Communications Center," [Online]. Available: http://www.swrcc.net/pages/about.php.

[31] Midlothian, Texas, "Northern Ellis Emergency Dispatch," [Online]. Available: http://www.midlothian.tx.us/index.aspx?NID=163.

[32] Cisco Systems, "Cisco ASA 5500 Series Adaptive Security Appliances," [Online]. Available: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html.

[33] D. Wessel, "Did 'Great Recession' Live Up to the Name?," *Wall Street Journal,* 2010.