

## Securing Tropo Wireless IP Broadband Networks

A TROPOS NETWORKS WHITE PAPER | AUGUST 2008

### Introduction

Wireless IP broadband mesh networks are being used increasingly in a wide variety of applications and vertical markets, including public safety mobility, video surveillance, automated utility meter reading and infrastructure (AMR/AMI), intelligent transportation systems (ITS), municipal modernization and mobility, automated parking meters, industrial control and communications, and public Internet access. Each of these applications and vertical markets presents its own, unique network security requirements.

To benefit network owners, operators and users, Tropo Networks has used its six-plus years of experience in deploying more than 500 customer networks to develop the technology and techniques necessary to meet the security requirements of multi-use, metro-scale broadband wireless mesh networks. Tropo's vast experience implementing networks for a wide array of applications and verticals uniquely positions the company to meet these diverse security needs.



It would be challenging enough to meet each of these security requirements if only one application or vertical used each network. However, wireless IP broadband mesh networks deliver the greatest return on investment (ROI) when multiple applications and classes of users share the same physical network infrastructure. As a result, deployment of multi-use networks is becoming commonplace.

Multi-use networks complicate the security picture by necessitating that the security requirements of all applications and classes of users be satisfied simultaneously. While there may be commonality of some requirements, the security needs of some applications and user groups may be mutually exclusive. For example, both the basic (e.g., use of WPA2 and SSID suppression) and advanced (e.g., use of VPNs and filters/firewalls that permit only VPN traffic to traverse the network) techniques that can be used to secure a public safety network cannot be used by public access networks where the network operator's business case depends on the ability of any standard Wi-Fi client to easily access the network.

This paper enables network administrators, network architects and CIOs to understand the multi-layer security approach that Tropos Networks has used successfully to secure hundreds of wireless IP broadband mesh networks. It also describes in detail how Tropos secures two of the most stringent applications – public safety mobility and video surveillance. Two sidebars are included – an in-depth look at how Oklahoma City is securing its multi-use municipal network as well as a discussion regarding differentiating metro-scale wireless security requirements from enterprise wireless security requirements and a cautionary note on wired security.



## Tropos' Multi-Layer Approach to Wireless Network Security

Tropos Networks has used its unparalleled experience in deploying metro-scale wireless IP broadband mesh networks to develop a multi-layer approach that achieves robust network security by leveraging time-tested and industry-proven techniques.

The task of securing wireless networks can be divided into five challenges:

1. Network access control
2. Network resource protection
3. End-point, including wireless client, protection
4. Secure end-to-end data traffic transmission
5. Secure network configuration, operation and management

Tropos Networks security elements incorporate and extend industry best practices for securing wireless networks, resources and data. We implement only security algorithms that have been industry-proven and verified, and that have been shown to be appropriate for metro-scale wireless IP broadband mesh networks. The principles used to craft our security approach include:

- Multi-layer – Utilize multiple security mechanisms at several network layers to provide high levels of protection.
- Time-tested and proven – Utilize well-known security techniques that have undergone extensive scrutiny by the security community and can offer users a strong degree of confidence in their implementation.
- Open, standards-based – Integrate open, standard elements so that a wide variety of economical clients and end-devices can securely attach to the network.
- Upgradeable – Incorporate upgradeability into products so that future security threats can be countered quickly via new software loads.
- Flexible – Accommodate the security requirements of the different applications and user communities sharing the network such that ROI can be maximized.

Each of the advanced security techniques employed in the Tropos Networks security model satisfies these design criteria. Techniques, protocols and algorithms such as traffic filtering, WPA2, EAP, RADIUS, AES, HTTPS, and VPNs have been employed for many years in a wide variety of Internet applications. Leveraging the higher-layer intelligence of our products, Tropos combines the best Internet and wireless security techniques to offer a robust and multi-layered security framework. No other wireless networking product combines all these elements to offer the highest levels of protection.

In the following sections, we will outline how the Tropos security features operate to secure the wireless network for even the most stringent operator requirements.



## 1. Network Access Control

Wireless network security begins with prohibiting access by unauthorized wireless devices while ensuring that authorized clients can connect reliably. Tropos MetroMesh routers support a wide variety of network access control mechanisms that can be tailored to meet a broad range of access control requirements.

### Wi-Fi Protected Access 2 (WPA2) Authentication

WPA2 is the Wi-Fi Alliance's latest security standard. It defines both authentication and encryption mechanisms, providing an interoperable implementation of the IEEE's 802.11i security standard.

WPA2 uses port-based access control built on IEEE 802.1x. Tropos Networks supports 802.1x authentication using the Extensible Authentication Protocol (EAP) and RADIUS. EAP supports multiple methods including PEAP, EAP-TLS and EAP-TTLS. Additionally, authentication and access control can be based on the use of Pre-Shared Keys (PSK).

Note that WPA2 authentication cannot be used in public access networks where network operators want new users to be able to register via the wireless network.

### MAC Address Access Control Lists (ACLs)

MAC address Access Control Lists (ACLs) provide additional protection when used in conjunction with other Layer 2 security mechanisms.

Tropos MetroMesh routers support the creation and administration of ACLs based on client MAC addresses. These ACLs can be whitelists and/or blacklists.

Creating a MAC address whitelist will allow only specific client MAC addresses to connect to the wireless network. Client MAC addresses not on the whitelist will not be able to connect to the network.

A MAC address blacklist will deny specific client MAC addresses the ability to connect to the wireless network. When a blacklist is employed, only client MAC addresses not on the blacklist have the ability to connect to the wireless network.

MAC address whitelists and blacklists can be created and administered from the Tropos Control element manager. Tropos Control centrally manages whitelists and blacklists and provisions them onto the Tropos MetroMesh routers.

Because hackers can spoof the MAC address of a valid client, MAC address-based authentication can be only one element of a layered security architecture.

Note that MAC access control whitelists cannot be used in public access networks where network operators want new users to be able to register via the wireless network.

MAC access control blacklists are suitable for all types of wireless IP broadband mesh networks.



### **SSID Suppression**

Wi-Fi access points typically broadcast their Service Set Identifier (SSID) (their network name) to allow client devices to discover the network. For networks where public access is desired, this is an essential function, altering potential users of the network's availability. However, for a private network, that is, one where access is limited to a specified set of users who already know of its existence, SSID broadcast is undesirable because it announces the network's availability to unauthorized persons.

Tropos MetroMesh routers allow network administrators to optionally suppress SSID broadcasts. In a private network, this does not hamper user access because client devices can be configured to attach to the network even though the SSID is suppressed. Suppressing the SSID broadcasts means that unauthorized persons will not know the network is available unless they use sniffing tools.

SSID suppression has been shown to be vulnerable to passive attacks, and is therefore considered inadequate if used alone. However, it is useful as a deterrent because it prevents a casual hacker from quickly accessing the wireless network.

Note that SSID suppression cannot be used in public access networks where network operators want new users to be able to register via the wireless network.

### **Per-User Group Authentication Policies Using Multiple VLANs and SSIDs**

To provide operators the flexibility to accommodate multiple classes or groups of users with differing wireless settings and security needs, Tropos MetroMesh routers support multiple virtual LANs (VLANs) and SSIDs with per-VLAN/SSID security configuration support.

Using this functionality, a single physical infrastructure can be used to set up multiple virtual network infrastructures offering different authentication methods and policies for different user communities. Each SSID/VLAN combination acts as a separate virtual network that is segregated from the other SSID/VLAN combinations through an amalgam of physical and network layer separation mechanisms, including distinct authentication profiles.

The use of multiple SSIDs mapped to distinct VLANs is one of the most prevalent and industry-standard building blocks for a secure multi-use wireless IP mesh network. As such, multiple VLAN/SSID support is required in all multi-use wireless IP broadband mesh networks.

Beyond security, multiple VLANs/SSIDs can also be used to ensure that high-priority users such as public safety officers receive access precedence and reserved bandwidth in the event of incident or emergency.



### **IP Address, Protocol and TCP/UDP Port Filtering for Access Control**

Packet filtering firewalls have long been used in conventional wired network security architectures. Tropos Networks has extended the concept to metro-scale wireless mesh networks with packet filtering capabilities that enhance wireless network security.

Tropos MetroMesh routers can filter traffic at the edge of the wireless networks using filters based on IP source and destination addresses, protocol and TCP/UDP port. For instance, if wireless access is permitted only for a specific set of clients for web browsing and e-mail, only traffic matching that profile will be forwarded by the Tropos MetroMesh routers. That is, only traffic from defined IP addresses or subnets destined to defined TCP ports (TCP port 80 for HTTP, port 110 for POP3, in our example) will be forwarded. This means that access can be controlled by application and by protocol, as well as by client. These policies will be enforced at the very edge of the wireless network.

Filtering is suitable for all types of wireless IP broadband mesh networks. However, care must be taken when configuring the filters to ensure that legitimate users and applications are not prevented from accessing the network.

### **Virtual Private Networks (VPNs) Combined with Filtering for Access Control**

To provide the highest levels of security, Tropos Networks recommends the use of industry-tested virtual private networks (VPNs). While the main function of a VPN is to provide secure end-to-end data transmission (see below), VPNs also play a role in network access control. When a VPN is used, only clients with the appropriate VPN software or hardware/software and valid login credentials can access the network, especially when combined with intelligent traffic filtering that permits only VPN traffic to traverse the network.

Note that traffic filtering as a means of requiring VPN use cannot be employed in public access networks where network operators want new users to be able to register via the wireless network.

## **2. Network Resource Protection**

Because wireless networks provide access to shared network resources (e.g., servers, printers, databases) and the network itself is a shared resource, wireless network deployments must protect network resources from malicious wireless users and others who would seek to do harm. Tropos MetroMesh routers accomplish this through a combination of physical deterrents as well as address, protocol and port filtering, alone and in conjunction with VPNs.

### **Physical Deterrents**

Tropos MetroMesh routers are equipped with indicators that provide evidence of tampering if any occurs. Further, a variety of software alarms sent to the Tropos Control element manager can alert network operators if any physical tampering takes place.



MetroMesh routers are FIPS-certifiable and include protections such as an encrypted file-system to guard and protect sensitive stored data.

These physical deterrents, when combined with a FIPS 140-2 certified VPN, can be used to create an end-to-end system that is FIPS 140-2 certifiable.

### **Address, Protocol and TCP Port Filtering for Network Resource Protection**

In addition to playing a role in network access control, packet filtering on Tropos MetroMesh routers also plays a part in protecting shared assets.

Returning to our previous example, destination IP address filtering can be configured on Tropos MetroMesh routers, in addition to IP source address and TCP port filtering. In this manner, authorized clients can not only be limited to web browsing and e-mail but also limited to connecting to specific web and e-mail servers. Crafting filters that disallow traffic to unprotected/ unauthorized wired or wireless hosts helps protect those assets. Again, the policies will be enforced at the very edge of the wireless network.

These measures are suitable for all types of wireless IP broadband mesh networks but must be carefully implemented.

### **VPNs Combined with Filtering for Network Resource Protection**

VPNs and the filtering capabilities of Tropos MetroMesh routers can help protect shared assets. Configuring filters that block all traffic except VPN traffic will prevent unauthorized traffic from reaching shared assets.

Again, traffic filtering as a means of requiring VPN use cannot be employed in networks where operators want new users to register via the wireless network.

## **3. End-Point, Including Wireless Client, Protection**

Wireless clients must be protected both for their own sake and to prevent a permitted client from being used for network access by an unauthorized client. This is especially important because wireless clients are not limited to human-operated devices such as laptops and PDAs – they also include automated end-points such as surveillance cameras, automated utility meter reading concentrators and wireless parking meter kiosks.

### **Multiple VLANs plus WPA2 for End-Point Protection**

Segregating different groups of users onto different VLANs protects end-points because only members of a given group can send traffic directly to other members of that group. This protection can be strengthened by requiring that WPA2 authentication be used to access the group's VLAN.

While multiple VLANs can be used in all wireless IP broadband mesh networks, WPA2 cannot be used in public access networks where network operators want new users to be able to register via the wireless network.



### **Evil Twin Detection**

Evil twin is a term used to describe an access point or wireless router that is configured with the same SSID as a wireless IP broadband mesh network but that is not actually a part of that network.

The intent behind an evil twin is not always malicious – for example, an enterprise may set up an evil twin to prevent their employees from connecting their work computers to a nearby metro-scale wireless mesh network. However, such an evil twin can have the unintended but undesirable effect of denying access to subscribers of the wireless IP broadband mesh network.

In other instances, evil twins are just that – evil, used for nefarious purposes such as harvesting passwords and other confidential information.

No matter why an evil twin is present, it is essential for network security that the network operator knows of its existence so that appropriate action can be taken. Tropos MetroMesh OS with Mesh Edge Service Management (MESM) supports configurable evil twin detection, enabling mitigation of evil twin threats.

Evil twin detection is required in all wireless IP broadband mesh networks.

### **Address Filtering to Block Peer-to-Peer Traffic Flows**

In the same manner that filtering can be used to protect shared network resources, it can also be used to protect wireless clients. In particular, IP destination address filtering on Tropos MetroMesh routers can be used to prohibit wireless clients from sending traffic to other wireless clients.

This type of filtering is suitable for all types of wireless IP broadband mesh networks. Note, however, that it may disable some peer-to-peer applications where both peers connect to the wireless network.

### **VPNs Combined with Filtering**

As described previously, Tropos MetroMesh routers can be configured to permit only VPN traffic to enter the network and to force that traffic to go only to specified VPN servers on the wired network. A by-product of this configuration is to protect wireless clients because no traffic can be sent directly to them from the wireless network.

### **Use of Embedded Web Servers with SSL**

While beyond the scope of security provided by Tropos MetroMesh routers, it is important to note that many wireless end-points that are not human-operated devices (e.g., wireless video surveillance cameras) contain embedded Web servers. To ensure maximum security, if these Web servers are used, they should be configured to always employ Secure Sockets Layer (SSL), aka, HTTPS.



#### 4. Secure End-to-End Transmission

Whenever possible, wireless network traffic must be shielded from eavesdroppers using a strong encryption algorithm.

##### WPA2 Encryption for Client-to-Mesh Router Links

In addition to providing access control via standardized authentication mechanisms, WPA2 also defines encryption between the client and the access point or mesh router using AES or TKIP ciphers. These provide for dynamic per-user encryption keys that are derived per-session as part of a key negotiation process. Tropos MetroMesh routers support both TKIP and AES ciphers.

WPA2 is necessary but not sufficient to ensure secure end-to-end transmission. Encryption of mesh traffic is also required (see below.)

WPA2 cannot be used in public access networks where network operators want new users to be able to register via the wireless network.

##### SSL

As noted above, WPA2 cannot be used in public access networks where the operator wants new users to be able to register via the wireless network. As a result, users must take care to ensure that SSL is used to secure their transmissions when they send personal information over the Web. Use of SSL is indicated by the appearance of https:// (as opposed to http://) at the beginning of the address line in the user's Web browser.

Use of SSL to secure transmission of personal information on the Web is recommended at all times.

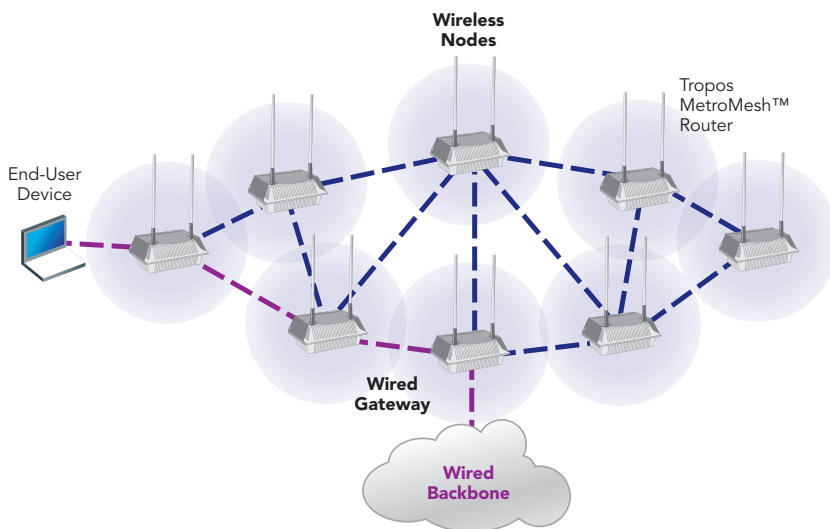


Figure 1: Basic Tropos Network Architecture

##### AES Encryption for Mesh Links

AES-encrypted mesh links contribute to secure data transmission. Tropos Networks uses AES to encrypt all data traffic through the mesh, across multiple hops, until the traffic reaches a wired gateway. (See Figure 1.) AES is recommended by the United States National Institute of Standards and Technology (NIST) as the most robust private key encryption technique.

AES encrypted mesh links should be used in all types of wireless IP broadband mesh networks.

##### Multiple VLAN Support for Secure Transmission

Tropos MetroMesh routers support multiple VLANs with per-VLAN security configuration. Using this functionality, a single physical infrastructure can support different user communities



with the traffic for each user community effectively segregated from that of all other user communities.

Multiple VLAN support is required in all multi-use wireless IP broadband mesh networks.

### **VPNs**

To provide the highest levels of security, Tropos Networks recommends and uses industry-tested virtual private networks (VPNs). VPNs are very challenging or impossible to overcome even when attacked by serious and sophisticated adversaries. In fact, the use of a VPN alone may be the simplest way to meet many security requirements, including FIPS 140-2 compliance, in a Tropos MetroMesh network.

Building on the lower layer methods we've already discussed, Tropos Metro-Mesh routers combine unique VPN compatibility and traffic filtering with industry-leading VPNs.

As enterprises began allowing employees to connect to internal networks via the Internet, VPNs were developed in response to the security threats posed by malicious hackers attempting to gain access to internal network resources. Connections from the Internet to the internal network are encrypted by the VPN once the user requesting the connection authenticates successfully. Other incoming connections are disallowed. Driven by the increasing popularity of remote corporate access over Internet links, VPNs have rapidly matured.

Today, connecting wireless networks to an existing wireline network poses risks similar those encountered when first connecting to internal networks via the Internet. Because wireless signals propagate far beyond the physical confines of the typical data network, wireless connections to the wired network also become a potential access method that can be exploited by malicious hackers.

Because of this threat, Tropos Networks strongly recommends using VPNs with metro-scale wireless mesh networks. VPNs (typically based on IPSec) are available from numerous vendors and offer proven implementations of network access control and secure data transmission. Tropos MetroMesh routers have demonstrated compatibility with a number of commercially available VPNs, including those from Cisco and NetMotion.

## **5. Secure Configuration, Operation and Management**

In addition to securing data transmission, it is also crucial to secure the configuration and management of the network infrastructure and safeguard its operation. Only authorized network operators must be able to alter the operation of network elements or the network's path selection protocol.

The techniques described below combine to enable secure configuration and management by preventing unauthorized access to, or monitoring of, the network's management and control traffic by malicious third-parties.



### AES Encryption for Mesh Links

In addition to the role AES encryption plays in securing data transmission, Tropos Networks also uses AES to encrypt the Predictive Wireless Routing Protocol (PWRP™), the protocol used by the MetroMesh routers to transmit node identification and path selection information to each other, as well as management information sent wirelessly from nodes to their associated gateways. (See Figure 2.)

AES encrypted mesh links should be used in all types of wireless IP broadband mesh networks.

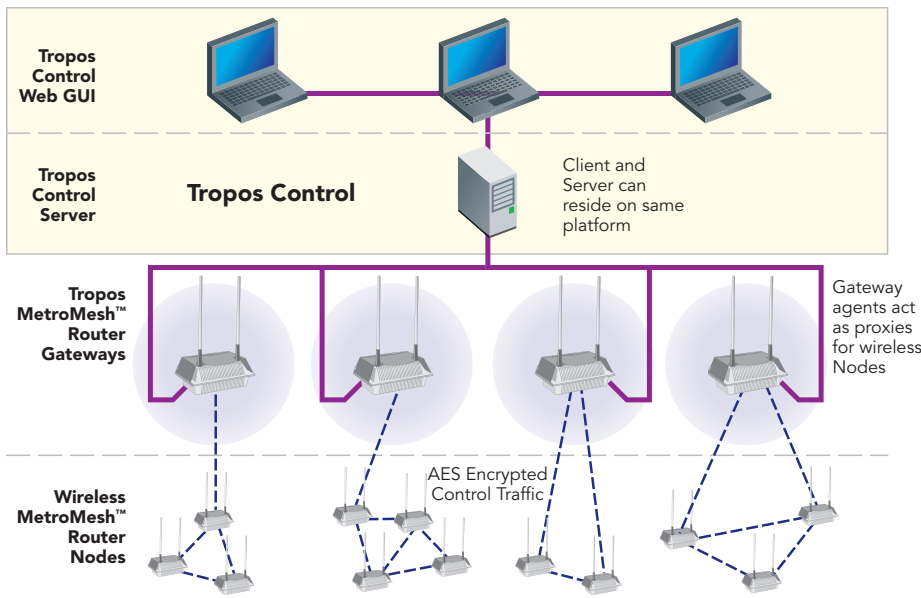


Figure 2: Secure Configuration and Management

### No Tropos Control Access from Wireless Clients

Tropos Control servers cannot be accessed via the wireless network. This prevents malicious wireless users from attempting to break into the Tropos Control server.

### Tiered Access Rights and Auditing for Tropos Control

To provide both the flexibility and security required for effective and efficient network management and administration, Tropos Control offers tiered access rights based on user type or function. Four levels of access have been defined for Tropos Control – Super-Admin, Admin, Read/Write and Read-Only. Authorization can be done locally on the management system or remotely using RADIUS.

Further, all configuration changes made to and/or using Tropos Control are logged, including time, date and user information. This provides an audit trail detailing who made what configuration change and when they were made.

### Secure MetroMesh Router Configuration

In addition to configuration via Tropos Control, Tropos MetroMesh routers can be configured and monitored by a web-based configurator. All configurator traffic is protected with HTTPS (see Figure 3). Network administrators can securely monitor and configure individual MetroMesh

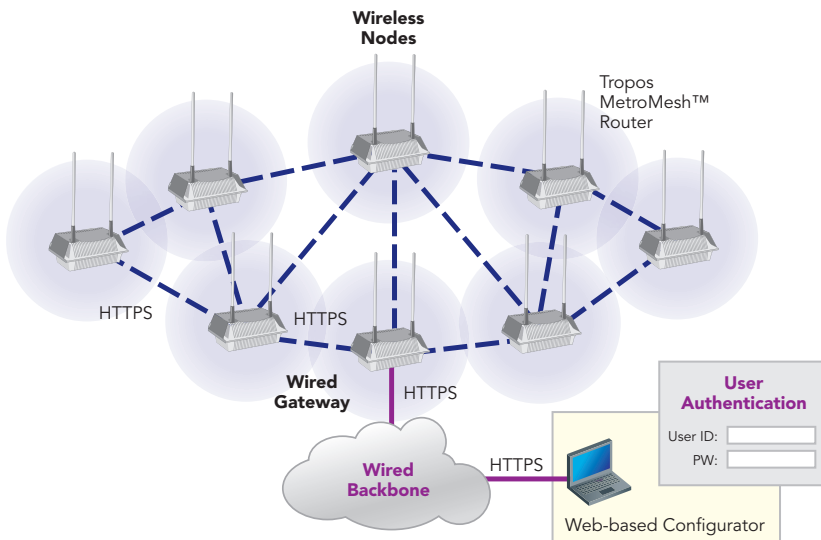


Figure 3: Secure Web-Based Configuration



## Case Study: Securing Oklahoma City's Network for Public Safety and Municipal Field Workers

Tropos MetroMesh routers support the strong, multi-layer security mechanisms specified by Oklahoma City, enabling end-to-end security. The 555 square mile Tropos MetroMesh network supports different user communities including police officers, fire fighters, building inspectors and public works employees. A user's login determines what security measures are required, their class of service, and which applications they are entitled to use. For example, a fire captain on his way to a situation can access video cameras in the area, and network traffic associated with this application will have higher priority than other non-essential traffic. Conversely, a public works meter reader does not have access to video surveillance applications.

Oklahoma City's security technologies and policies have worked well, protecting the network and delivering the performance needed for each user and application. Security technologies include:

- Tropos-enabled 802.1x authentication and key management, which supports EAP and Transport Layer Security (TLS).
- Tropos-enabled AES encryption for all end-user data traffic through the mesh, across multiple hops, until the traffic reaches a wired gateway.
- Tropos-enabled port filtering allows only that application-specific network traffic approved for a unique login.
- VPNs and firewalls also control network access and secure data transmission.
- Tropos-enabled AES encryption for all management traffic related to the Tropos MetroMesh.
- FIPS 140-2 compliance through the implementation of a FIPS 140-2 VPN (NetMotion).

routers from anywhere on the Internet. Login is provided by a certificate-based authentication scheme that can support up to 20 authorized users.

As with Tropos Control, all changes made using the configurator are logged, providing an audit trail.

## Network Security Application Examples

We now examine the mechanisms used to secure metro-scale wireless IP broadband mesh networks in two of the most stringent applications, public safety mobility and video surveillance.

### Public Safety Mobility

Because officers cannot tolerate interception or interference with public safety communications and because much of the information accessed by public safety employees in the field is highly confidential, the security requirements for public safety mobility applications are among the most stringent to be found anywhere. As a result, public safety mobility networks generally employ all of the techniques described in this white paper.

In some cases, such as the California Law Enforcement Telecommunications System (CLETS), the security precautions of the law enforcement agency using the wireless network must be approved before wireless access to databases and other information sources is permitted. For CLETS in particular, any data transmitted on an "untrusted" network, e.g., the Internet or a wireless network shared by the public, even if public access is provided on a VLAN different than the one used by law enforcement, must be encrypted and the agency must provide to CLETS for their approval a diagram of the network showing how the untrusted portions are encrypted.

However, the current trend is away from specific security requirements. Instead, organizations that maintain public safety databases sign agreements with the chief law enforcement officer of agencies wishing to access the databases. In these agreements, the chief law enforcement accepts responsibility to prevent unauthorized database access via his agency's resources. Compliance is ensured by periodic audits. This process is used, for example, by the National Crime Information Center (NCIC) and the Texas Crime Information Center (TCIC).

To ensure security, many public safety agencies use WPA2 to provide a base level of encryption and authentication, MAC address whitelists to help ensure that only authorized clients gain access to the network and SSID suppression to keep from openly announcing the network's existence. Multiple VLAN/SSID use is required to ensure that employees of different public safety agencies can access only their own agency's resources. For instance, NCIC access may be permitted for sworn law enforcement officers but prohibited for emergency medical technicians (EMTs). On the other hand, EMTs may be permitted to see medical records that may not



be accessed by law enforcement officers per Health Insurance Portability and Accountability Act (HIPAA) regulations.

VPN usage is required for virtually all public safety mobility applications and the ability of Tropos MetroMesh routers to use filters to restrict network usage to VPN traffic is often used to increase the network's hardness. Also, by using a FIPS 140-2

certified VPN in conjunction with Tropos Metro-Mesh routers, requirements to meet the standards of FIPS 140-2 – common in public safety environments – can be satisfied in the metro-scale wireless network environment.

Many public safety agencies further harden their networks, augmenting the security provided by Tropos MetroMesh routers with non-Tropos solutions such as intrusion detection systems, which are beyond the scope of this white paper.

The results have been impressive. For example, the City of Corpus Christi's (Texas) has passed four TCIC and two NCIC audits since its police department began to use the city's metro-scale wireless network.

### Video Surveillance

The requirements for securing video surveillance networks are similar to those for public safety networks with a twist – many end-points on the wireless network are surveillance cameras that may not be equipped with the same security facilities as laptops, handhelds and other human-operated devices. All of the techniques discussed in the section regarding mobile public safety applications should also be used for video surveillance. Additionally, several special considerations must be taken into account when securing wireless video surveillance networks.

One consideration is how the surveillance cameras will be connected to the network. To both minimize network traffic and enhance security, the preferred mechanism is to connect cameras directly to an Ethernet port on a Tropos MetroMesh router. With this method, there's no possibility of wirelessly snooping the hop between the camera and the router because there is none. Further, all surveillance camera traffic between the router and

## Metro-Scale and Enterprise, Wireless and Wired

While there is some commonality between the basic security requirements for enterprise WLANs and metro-scale wireless IP broadband mesh networks, there are also significant differences. Further, some techniques required for enterprise WLAN security are unnecessary or inappropriate for metro-scale networks and vice versa.

For example, the ability to detect and disable rogue access points (APs) is crucial for ensuring enterprise security. However, in metro-scale deployments, it is expected that the wireless network and its users will be within range of possibly hundreds of access points belonging to other, perfectly legitimate networks. Any attempt to disable these access points would run afoul of regulations in most countries of the world, not to mention common courtesy and sense.

Another consideration is the fundamental architecture of the wireless network.

Most enterprise WLANs use a thin AP/central controller architecture. This makes sense because the only wireless hop is the one between the client and the AP and the WLAN controller can reside on the LAN switch that is required to connect the Ethernet links from the various APs.

In metro-scale wireless broadband mesh networks, data may need to traverse several mesh links between wireless routers before arriving at the wired network. The bandwidth on mesh links is a precious commodity, one that must not be squandered. It makes no sense to force traffic to traverse wireless links to an expensive, failure-prone, centralized controller only to be dropped because of security concerns. To the contrary, a central controller architecture opens metro-scale wireless networks to denial of service (DOS) attacks by failing to stop malicious packets at the network's edge.

Rather than a central controller architecture, it is crucial that metro-scale wireless IP broadband mesh networks detect threats and enforce security policies at the edge of the wireless network. Doing so saves valuable airtime, increasing the usable capacity of the entire network.

When securing metro-scale wireless networks, it is crucial to insure that the wired networks to which they connect are also secure. Only someone in the physical vicinity of a wireless network is a potential intruder – a population that generally numbers in the hundreds or, at worst, in the thousands. Contrast this to wired networks that connect to the Internet. Anyone with a computer and an Internet connection is a potential intruder – a population that numbers in the hundreds of millions!

For some applications such as public safety mobility, there may be a temptation to adopt a brute force approach to this problem and physically separate the wired network that serves as the back-end for the wireless network from the wired network that connects to the Internet. This approach denies Internet access via the wireless network.

While tempting, this approach significantly limits the utility of the wireless network. As one former law enforcement officer told Tropos, "Federal and state databases such as NCIC (National Crime Information Center) generally contain information only about career criminals. The Internet provides officers in the field with much more information about people who are just beginning their life of crime."

The best approach is not to disable Internet access but to provide solid security for the wired network and its connection to the Internet.



the wired network will be secured by AES. If this is not possible, the second best choice is to use a Wi-Fi CPE external to the camera to create the client side of the camera-to-router hop. Appropriate Wi-Fi CPEs come with built-in encryption and firewalls that can be used to secure the camera and its video traffic. The least desirable method of connecting the camera is to insert a Wi-Fi card into a PC Card slot in the surveillance camera. Wi-Fi cards normally have only basic security features such as WPA2.

Professional-grade IP security cameras have built-in, configurable security features. These include password access control and firewalls that can be set up to restrict access to only specified users or servers. It is therefore imperative that the video surveillance system is set up to provide strong access security to augment the wireless network's security.

The most important consideration is to control how the video streams are distributed to users of the system. All IP cameras include an embedded web server that can, by default, be accessed by any authorized user on the network. However, the preferred mechanism is to utilize the cameras' built-in firewalls to prohibit such access and distribute video streams only through the network video recorder (NVR) servers. Access to live (and recorded) streams for mobile security personnel is then facilitated through the re-broadcast and control mechanisms of the servers themselves. Again, this minimizes network traffic and enhances security, allowing the implementation of role- and function-based access and control policies.

In some instances, it may be desirable to co-locate the NVR with the video camera(s). For example, if video cameras are mounted at an intersection with a traffic signal, it might be possible to place the NVR in the cabinet that houses the switching equipment for the traffic signal. This placement further enhances the security of the cameras' feeds and reduces that amount of wireless network traffic between the cameras and central location where the NVRs are aggregated.

## Summary

By leveraging the inherent intelligence of its MetroMesh routers, Tropos Networks combines the most rigorous Internet security techniques to offer a robust and multi-layered security framework.

This security framework can be configured to suit a broad range of access strategies, from the relatively unrestricted public access with minimal deterrents required by a wireless ISP, to the totally secure private network needed for law enforcement and other public safety applications.



Using this multi-layer approach, network administrators have at least three tools they can use to secure each of the five main areas of concern in wireless networks. See Figure 4.

A final advantage of the Tropos security approach is upgradeability.

New security threats are emerging constantly. Tropos continually incorporates new techniques for combating threats into its MetroMesh routers. Because Tropos MetroMesh routers are very intelligent, and most security features are implemented in software, MetroMesh routers' security features can be enhanced with new releases of Tropos MetroMesh OS, the Tropos network operating system.

|  | Network Access Control | Network Resource Protection | End-Point Protection | Secure Data Transmission | Secure Configuration, Operation and Management |
|--|------------------------|-----------------------------|----------------------|--------------------------|--|
| Physical Deterrants                    |                        |                             |                      |                          |  |
| WPA 2                                  |                        |                             |                      |                          |  |
| MAC ACLs                               |                        |                             |                      |                          |  |
| SSID Suppression                       |                        |                             |                      |                          |  |
| Multiple SSID Support                  |                        |                             |                      |                          |  |
| Multiple VLAN Support                  |                        |                             |                      |                          |  |
| Address, Protocol and Port Filtering   |                        |                             |                      |                          |  |
| VPNs                                   |                        |                             |                      |                          |  |
| VPNs Combined with Filtering           |                        |                             |                      |                          |  |
| Evil Twin Detection                    |                        |                             |                      |                          |  |
| AES Encrypted Mesh Links               |                        |                             |                      |                          |  |
| No Tropos Control Access from Wireless |                        |                             |                      |                          |  |
| Tiered Access Rights                   |                        |                             |                      |                          |  |
| Secure Configuration                   |                        |                             |                      |                          |  |
| Auditing                               |                        |                             |                      |                          |  |

Figure 4: Tropos Meeting the Security Challenge

## About Tropos

Tropos Networks is the market leader in delivering metro-scale wireless mesh network systems with more than 500 customers in 30 countries around the world. The patented Tropos MetroMesh™ architecture delivers the ultimate scalability, high capacity at low cost and great user experience demanded by enterprises and network users. Tropos Networks' unique expertise includes high reliability and performance mesh software development, mesh RF engineering, metro-scale network planning, deployment and optimization, and navigating the municipal approval process. Tropos Networks is headquartered in Sunnyvale, California. For more information, please visit [www.tropos.com](http://www.tropos.com), call 408-331-6800 or email to [info@tropos.com](mailto:info@tropos.com).



555 Del Rey Avenue  
Sunnyvale, Ca 94085  
408.331.6800 tel  
408.331.6801 fax  
[www.tropos.com](http://www.tropos.com)  
[sales@tropos.com](mailto:sales@tropos.com)

© 2003-2008 Tropos Networks, Inc. All rights reserved. Tropos and PWRP are registered trademarks of Tropos Networks, Inc. Tropos Networks, MetroMesh, AMCE, TMCX, SABRE, CMDP, MESM and Metro-Scale Mesh Networking Defined are trademarks of Tropos Networks, Inc. All other brand or product names are trademarks or registered trademarks of their respective holder(s). Information contained herein is subject to change without notice. The only warranties for Tropos products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Tropos shall not be liable for technical or editorial errors or omissions contained herein.