Securing Mitel Cloud Based Unified Communications (UC) Networks

MITEL SOLUTIONS ENGINEERING GROUP

Technical Paper

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

TRADEMARKS

Securing Mitel Cloud Based UC Networks
Mitel Solutions Engineering Group – Technical Paper
Version 1.0

Chapter 1 Overview

The purpose of this document is to provide interested parties with recommendations on how to ensure that the Mitel Cloud based Unified Communications (UC) solutions are protected from security threats.

This document discusses the Mitel Cloud based UC solution operational models, the network security challenges that are presented when Mitel UC solutions are deployed in the Cloud, and how a shared responsibility security model is required to address the UC security requirements.

The network designer and system administrator are provided with general recommendations for network architecture and security, the document then delves into detailed recommendations and best practices for securing Mitel Cloud based UC solution networks, specific areas discussed are:

- How to secure the Access, Distribution and Core layers of the network
- Identification of the UC assets that require protection
- How to partition the network into varying levels of trust - network trust zones
- Use of next generation security tools to provide security controls between the trust zones
- UC Network Security models and diagrams
- How to ensure that the network security tools are working in unison

This document is part of a suite of Mitel security documents that discuss topics related to Cloud based UC security, the documents included in this suite are:

- Securing Mitel Cloud Based UC Networks
- Network Intrusion Detection and Intrusion Prevention Systems

Chapter 2 Introduction

Currently available next generation security tools provide the network designer with powerful tools to help secure the network, but they are only one aspect of a total security solution. The network designer and administrator also need to be aware that overall network security is a responsibility that is shared between service providers, application providers, users and network administrators; this subject is discussed in Cloud Operational Models and Shared Responsibilities for Security.

In some sections, this document uses the MiCloud Business Solution Medium large Business (MLB) and the Enterprise UC Solution Private Cloud reference architectures to show how next generation security tools might be applied, however these reference architectures are used only for illustrative purposes.

The principles discussed in this document are generic in nature and can be applied to other UC solution architectures, with the exception of Mitel's Cloud based Contact Centre Solutions and all multi-tenant Cloud architectures, these solutions are outside the scope of this document.

For detailed information on how to secure a particular UC solution contact Mitel Professional Services.

Who are the Parties that Should Use this Document

There are a number of different operational models that may be used for delivering Mitel's Cloud based UC solutions to an end customer.

The various operational models involve multiple parties that work together to provide the UC solution. Each of these parties is responsible for ensuring the security for their part of the solution and as a result, each of these parties may benefit from consulting this document.

The parties that might be involved in delivering Mitel's Cloud based UC solutions are:

- Infrastructure as a Service providers (IaaS)
- Platform as a Service providers (PaaS)
- Software as a Service providers (SaaS)
- Unified Communications as a Service providers (UCaaS)
- Mitel Unified Communication solutions resellers
- Mitel Partners
- End customer administrators and security/IT personnel

Identifying the parties that are involved in operating the UC solution, and identifying your organization's role will help the reader focus on the parts of this document that are relevant to their field of responsibility.

For further information on the various operational models, the parties involved, what their security responsibilities are, and how they relate to Mitel's UC solution, refer to the section of this document called Cloud Operational Models and Shared Responsibility for Security.

This document will be of interest to the following parties:

- End customers that are moving their UC services to an Enterprise UC Solution, using private cloud reference architecture.
- End customers that are migrating their UC services to a MiCloud Business Solution, using UCaaS deployment
- End customers that are using Cloud based UC solutions
- UC resellers that are expanding their business into the UCaaS business
- UCaaS Providers with their own infrastructure, that are looking to improve their infrastructure security
- UCaaS Providers without their own infrastructure, that are evaluating IaaS providers and the security capabilities of IaaS providers

How to Use This Document

This document focuses on how to use next generation security tools to help secure the Mitel UC Solutions. The principles discussed are generic in nature, and are not specific to a particular UC solution reference architecture.

The MiCloud Business Solution Medium Large Business (MLB) reference architecture and the Enterprise UC Solution Private Cloud reference architecture are used in this document for illustrative purposes to show how next generation security tools might be applied.

It is recommended that the reader should be familiar with the UC solution that they are interested in securing, the components and applications involved in building the UC solution, and how they are networked together.

For detailed descriptions of the UC solutions and topologies, refer to the following Mitel documents, which can be found on Mitel on Line:

- MiCloud Business Solutions are described in the *MiCloud Business Solution Blueprint*.
- Enterprise UC Solutions are described in the *Enterprise UC Solution Blueprint*.

This document has been structured into chapters that cover very specific topics. These chapters can be grouped into three basic categories; tutorial or background information, recommendations on how to secure a Mitel UC solution, and information related to selecting, deploying and maintaining security tools.

- Chapters 2 and 3 provide background and tutorial information, and will be useful to individuals who are not familiar with public or private Cloud deployments, Cloud security risks or hierarchical network design.
    - *Chapter 2 Cloud Operational Models and Shared Responsibilities for Security* discusses how Cloud services are delivered; the various operational models and what shared security means in the Cloud world.
    - *Chapter 3 Cloud Computing Presents New Security Challenges* discusses why traditional defenses are no longer adequate for Cloud based deployments, why Cloud deployments

are subject to new types of threats and the organizational and technical challenges related to ensuring Cloud security.

- Chapters 4, 5 and 6 focus on Mitel UC solutions and how to ensure the solution's security, these chapters assume that the designer is familiar with hierarchical network design and next generation security tools
  - *Chapter 4 Network Architecture & Security - Recommendations.* This chapter provides the reader with an overview on hierarchical network design practices, how different users and resources should be compartmentalized and discusses why networks designed in this way are inherently more defensible. This chapter also provides recommendations on network design and how security tools should be employed to secure the network.
  - *Chapter 5 Securing the UC Network* discusses how to secure the UC network, both, Cloud based and On-premise based solutions are addressed.
  - *Chapter 6 Unifying Next-Generation Security Tools* summarizes where security tools should be located, this chapter also discusses how next generation security tools can be part of defense-in-depth strategy.

Chapter 3 Cloud Operational Models and Shared Responsibilities for Security

There are a number of different operational models that can be used for delivering Mitel's Cloud based UC solutions to an end customer.

These operational models may involve multiple organizations that work together to provide the UC solution, or there may be one organization with several departments that are involved with providing the UC solution. In both cases, each organization or department is responsible for ensuring the security of their part of the solution. All of the involved parties should be aware that a comprehensive security solution is based on a shared responsibility model.

Further discussions pertaining to shared responsibility for security in the Cloud can be found at the Cloud Security Alliance, https://cloudsecurityalliance.org. The CSA document called Security Guidance for Critical Areas of Focus in Cloud Computing V3.0 is of particular interest.

Cloud Services - The Service Providers

Cloud service providers can be grouped into three broad categories: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

When planning for security, it is important to understand the roles of the Cloud service providers and the divisions of responsibilities between them for ensuring security.

The roles of the Cloud services providers and how they relate to the Mitel UC solution are as follows:

Infrastructure as a Service

Infrastructure as a Service (IaaS) is a term for a Cloud service that offers physical infrastructure such as buildings, power, environmental controls, and computing resources; this includes physical or virtual machines, storage and networking capabilities.

Customers of the IaaS provider install and manage their application software on the IaaS provider's Cloud infrastructure and the IaaS provider maintains the virtualized infrastructure and physical infrastructure.

An UCaaS provider might lease infrastructure services from an IaaS provider for hosting a MiCloud Business UC solution.

Platform as a Service

Platform as a Service (PaaS) is a term for a Cloud service that offers a complete solution including the middleware and operating system layers and in some cases applications, as well as any additional resources like storage and networking capabilities.

The PaaS provider may deploy multiple instances of the UC solution. The PaaS provider may then sell UC solutions directly to the end customer, who then pays the PaaS provider for UC services. Alternately, the PaaS provider may sell UC solutions to a virtual service provider, who in turn sells UC services to the end customer. The virtual service provider pays the PaaS service provider relative to the capacity they are leasing.

Software as a Service

Software as a Service (SaaS) is a term for a Cloud service that offers the end customer applications or functions as a service. The Mitel UC portfolio enables service providers to build SaaS offers ranging from basic voice-centric services to UC intensive services.

For example, an end-customer may require UC solutions for 30 employees. The end customer will pay the service provider every month for 30 extensions. Each extension includes voice-mail, presence, and instant messaging.

Unified Communications as a Service

Unified Communications as a Service (UCaaS) refers to a Cloud service provider offering where UC services are delivered to end customers directly from the Cloud. Depending on the operational models employed, UCaaS can be similar to a SaaS offering or similar to a PaaS offering.

- When an UCaaS provider is providing UC solutions directly to the end customer, the UCaaS offering is similar to a SaaS offering.
- When the UCaaS provider sells UC solutions to UC solution resellers, the UCaaS offering will be similar to a PaaS offering. Under this arrangement, the UC resellers then sell UC solutions to the end customer; the UC reseller may also manage the UC solution on behalf of their own end customers. Sometimes this business model is referred to as “Mitel built, partner managed”.

UC Cloud Solution Operational Model

The UC Cloud solution operational model is shown in Figure 1, this model will be used in this section to illustrate how security for Cloud solutions needs to be a shared responsibility.

The UC solution operational model shows the division of operational responsibilities between the various service providers, or the case of a single service provider, the various departments in the organization:

- The IaaS provider provides the physical infrastructure, the computing resources, the core connectivity infrastructure, and possibly the private network connectivity (e.g. MPLS).
- The PaaS or UCaaS provider is responsible for installing and administering the Cloud based UC solution applications onto the infrastructure provided by the IaaS.

- Depending on the role of SaaS provider and end customer's requirements, the SaaS will have varying degrees of responsibility for the UC end points that are located on the customer's premises.

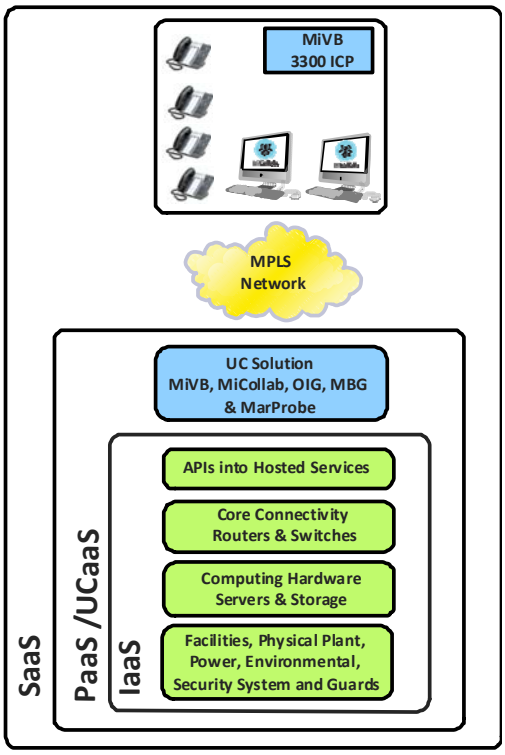

Figure 1 UC Solution Operational Model

The roles of the various service providers may not always align with the boundaries between IaaS, PaaS and SaaS as described above in the operational model.

Some service providers may be responsible for multiple roles. However, in most cases even if a service provider assumes multiple roles, these responsibilities will be divided up between different departments. For instance, one department manages the physical infrastructure; one department manages the UC applications and related platforms, and one department delivers end customer services.

What is important to consider, is that no matter which roles the service providers assume, all of the roles in the operational model remain necessary, and the service providers or departments responsible for a given set of roles must also be responsible for ensuring that the security requirements associated with these roles are met.

UC Cloud Solution Shared Security Model

Historically, when enterprises owned the entire networking infrastructure, they were responsible for network security.

With Cloud based solutions, the model for ensuring network security changes. When a customer migrates to Cloud based solutions, the end customer still bears some responsibility for security. However the Cloud introduces new divisions of responsibilities between the end customers and service providers.

With Cloud based solutions, the precise definitions of who is responsible for security present new legal and operational considerations.

Parties involved in delivering Cloud solutions, or parties utilizing Cloud solutions should ensure that contracts/SLAs have been established, and that the contracts clearly define each service provider's responsibilities and the end customer's responsibilities.

These contracts or SLAs will constitute a shared understanding of the overall security model.

Additional reading on this subject can be found in the Cloud Security Alliance document called Cloud Controls Matrix. This document can be found at - https://cloudsecurityalliance.org/

Chapter 4 Cloud Computing Presents New Security Challenges

Compared to traditional enterprise networking models, Cloud computing presents several new security challenges, these challenges are rooted in both operational and technical changes related to Cloud computing. These new challenges are discussed below.

Organizational Challenges to Maintaining Security

When enterprises had their entire networking infrastructure and all of their applications located on their own premises they were able to assume responsibility for their network and application security.

Now, as enterprises migrate to Cloud based applications and UC solutions, it is no longer possible for the business to have sole ownership of their security requirements - security becomes a responsibility shared amongst the various service providers involved in providing the overall Cloud solution.

Previously, organizations managed their network security through operational policies and technical solutions.

When an organization migrates to Cloud based applications, operational policies and technical solutions are still required to secure the network, but due to the fact that responsibility for security is now shared amongst the various service providers, securing the network also requires contractual solutions. These contractual solutions are discussed in the chapter called, Cloud Operational Models and Shared Responsibilities for Security.

Technical Challenges to Maintaining Security

Securing Cloud based networking and applications presents some new technical challenges compared to traditional premise based networking and applications.

The network perimeter was previously a well defined boundary. The company's assets were contained within a secure building and access to outside networks and branch offices was realized through well defined demarcation points, and network access was controlled with well defined rules. With Cloud based solutions, the network perimeter is very fluid; it is defined by the location of all applicable resources such as servers, data bases and also by wherever the users and their end points are located, or happen to be located on any given day.

Network designers need to recognize that when applications move from the premise to the Cloud, there is no longer a clearly defined network perimeter. The company's computing and communication assets can no longer be fully protected with traditional perimeter defense mechanisms, such as firewalls and DMZs.

When servers and applications reside off site in the Cloud, the company's data will flow outside of the company's premises and out of the company's immediate control.

Companies continuously need to implement better access controls for regular users, but more critically, for highly privileged users such as system administrators. If an unauthorized user manages to obtain the required information to pose as an administrator for a premise based network, the damage that can be done can be significant.

If such an individual is able to assume administrator privileges to a cloud based network, the damage that could be inflicted would be far worse. Cloud based networks make heavy use of virtualization technologies. When assets are virtualized, the assets are concentrated on one or more servers and the security risk to these assets is also concentrated. Virtualization can result in several types of data and several types of applications being co-located on one machine; it is also possible that multiple customers may be hosted on a single machine. This gives an unauthorized 'administrator' access to far more data and applications than in a non-virtualized environment. The damage that an unauthorized 'administrator' could inflict in a short period of time is immeasurable.

To address these new networking changes, network designers need to change the way they think about network security.

This document provides the reader with recommendations on how to secure Cloud based UC applications using widely accepted industry practices such as:

- Partitioning the network into different trusts zones
- Employing next generation security tools to segregate the trust zones an monitor traffic between the trust zones
- Creating a trust zone specifically for UC solution applications, end points and management data
- Employing next generation security tools to control network access for users and applications
- Incorporating a Security Information and Event Management solution (SIEM) into the network security management infrastructure
- Using NGFWs, SBCs and proxies for connections to untrusted video and audio end points

These practices are aligned with security recommendations that were published by Gartner in a February 2015 white paper called How to Secure Enterprise Voice and Video.

Cloud Security - Keeping Current

A Security Information and Event Manager (SIEM) is a critical part of the overall security solution. The SIEM should communicate with all of the security tools such as Intrusion Detection and Protections Systems, Next Generation Firewalls, Web Application Firewalls, etc.

The SIEM is responsible for obtaining security signature updates from the SIEM vendor's site and distributing these updates to the network security tools. Should a network security tool detect suspicious activity, it will notify the SIEM, if the SIEM receives multiple indications of suspicious activity, the SIEM will attempt to correlate the information, notify the administrator and the SIEM may take measures to try and contain the threat.

To keep security measures up to date it is imperative that a SIEM be incorporated into the network's security infrastructure and that subscription services for signature/security updates be maintained.

Where a very high level of protection from threats is required, the network designer may want to consider deploying two SIEMs with subscriptions services, and procuring the SIEMs and the subscription services from two different SIEM vendors. While this may be an expensive proposition, the benefit is that one subscription service may be aware of a threat before the other subscription service is aware of the threat.

The network administrator needs to recognize that keeping security measures up to date with security threats is a never ending game of cat and mouse.

Chapter 5 Network Architecture & Security – Recommendations

Network architecture can have a major influence on how secure a network is. Historically, networks were designed with performance, availability, maintenance and cost in mind. Network security was often designed in as an afterthought and the result was a piecemeal solution - leaving many potential security gaps. Today, networks must be designed with security considerations in mind right from the start.

When designing security into a network, focusing on perimeter defenses is very important, but it is not enough, the internal network also requires defense mechanisms. If an attacker or a piece of malicious code is able to gain access to one device connected to the interior of the network, perimeter defenses, which typically focus on inbound threats will have no ability to thwart an attack.

In very general terms, securing a network against attacks involves:

- **Securing network access**

  This involves securing network end points and devices, management interfaces and external access points. Physical network demarcation points should also be secured so that a network connection cannot be intentionally severed causing isolate part of the network to be isolated.

- **Ensuring that attacks can be detected and that action can be taken against attacks**

  Further information on this subject can be found in the Mitel technical paper - *Network Intrusion Detection and Intrusion Prevention Systems*

- **Limiting what can be attacked from inside or outside of the network**

  This is accomplished by architecting the network in such a way that when an attack does occur, it will be contained to a small area of the network, or the speed with which an attack spreads will be limited so that the impact on users and overall network functionality is minimized.

Architecting the network to achieve these goals is discussed in the following sections.

Hierarchical Network Design and Security

When designing a network the use of a hierarchical design should be considered. While hierarchical network designs offer many benefits that are unrelated to network security such as enhanced network availability, improved network maintainability and alignment with structured wiring practices - a hierarchically designed network is ideal for implementing network security controls and identifying network demarcation points.

Hierarchical network design has been an accepted design practice for on-premise based networks for many years, and hierarchical network designs are just as applicable to cloud based solutions. A hierarchal network design approach may be used in the cloud data centre and also on-premise at the end user's location.

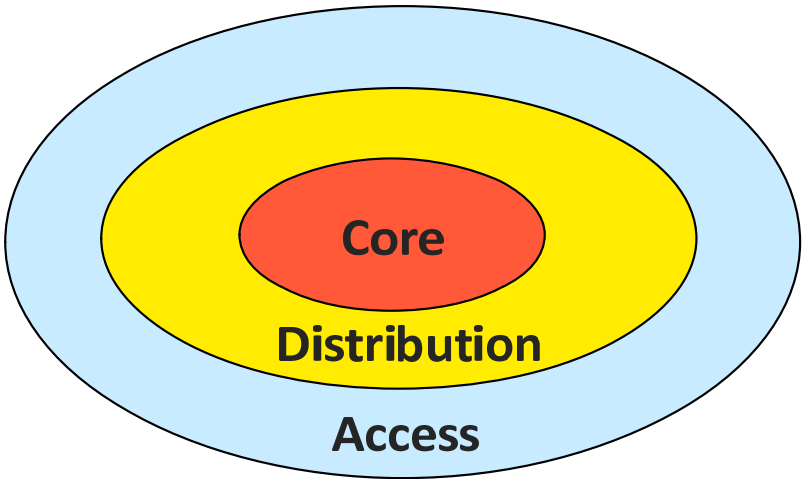

Figure 2 Hierarchical Network Layers

As shown in Figure 2, hierarchical networks are designed with three layers, the Core, Distribution, and Access layers. The components that comprise the network layers, what the layers connect to and where the layers are physically located are described below:

For an On-premise based network:

- The Core equipment will be located in a server room or the data centre room. The Core equipment connects Distribution switches to each other and provides connections to shared network resources such as servers, UC solutions, SIP gateways, WAN routers and internet gateways.
- The Distribution layer equipment will be located in wiring / telecommunications closets which are usually located on each floor of a multi-floor building, closets are also located in separate buildings within a campus. The Distribution layer equipment connects to the Core and Access layer equipment via high speed links. The Distribution devices are typically L2 ethernet switches. These L2 switches should be located in wiring closets where access to vertical riser conduits is available.

- The Access layer equipment will be located either in the wiring closets (preferred) or physically close to the work groups that require connectivity. This layer will connect end user devices such as IP phones and personal computers to the Distribution layer.

For a Cloud based network:

In Cloud based networks when there is significant amounts of networking gear located on the customer's premises, Distribution layer equipment might be located in both the Cloud data centre and on the customer premises.

For the case where the customer premise network extends into the cloud, the cloud is considered as part of the distribution network. For smaller deployments, the cloud may be the only part of the network, in which case it may fulfil both core and distribution roles. Customer VLANs may also be extended across the WAN link which may then separate out in the cloud for different service, e.g. VoIP to one location and business services in another location.

In summary, the main difference between on-premise and Cloud based hierarchical networks is:

- On-premise networks have the components from all of the layers of the hierarchy located on-premise.
- Cloud based networks will have the Core and Distribution layer components located in the cloud. But depending on how much networking equipment is located on the customer's premises, the Distribution layer components may be located in both the Cloud and the on-premise location. These two sets of Distribution layers components will connect to each other through a WAN or an internet connection.

How does a Hierarchical Network Design help with Security

As previously described, hierarchical networks divide the network into the three distinct layers, Core, Distribution and Access. A hierarchical design places the devices that are the most critical to protect in the Core, less critical devices in the Distribution layer, and the least critical devices in the Access layer.

Each layer of a hierarchical network aligns with a specific set of networking functions, and each set of networking functions requires unique types of security. This allows the designer to apply unique security measures to each layer of the hierarchy.

In conclusion: a carefully designed hierarchical network, in conjunction with the appropriate security tools, helps ensure that a security breach on one network level does not result in a succession of security breaches on other network levels.

Network Trust Zones and Security

Trust Zones - what are they?

A trust zone is an area within a network that is occupied by a group of users and devices with the same security requirements and networking characteristics, some examples of the shared characteristics are:

- Access controls
- Audit, logging and monitoring requirements
- Data confidentiality and integrity requirements
- Network availability
- Application availability
- Network privileges

A trust zone may cover a physical area, a logical area, a range of IP addresses, or all these criteria. A trust zone may also span different hierarchical network layers or be contained on one layer.

Trust zones will be separated from each other by routers or firewalls and the network designer will deploy a security device at these junctures between trust zones. The capabilities of the security devices that are deployed will depend on the security requirements for the users, devices and data contained in the trust zone.

Creating trust zones is an important step that the network designer must take while creating the network security model. Trust zones are put in place to:

- Control communication between trust zones
- Create a logical junction for monitoring inter-zone communications for security breaches
- Create a logical area of the network that can be isolated in the event of a security breach
- Identify a network segment that requires the same data confidentiality and integrity rules.

In summary, a trust zone will contain users, devices, applications and sections of a network that share all of the same security requirements.

How do you define a trust zone?

An important step in deciding how to create network trust zones, involves designing the network topology, or in brown field situations - redesigning the network topology.

There are two perspectives to keep in mind when viewing and designing a network topology, the physical topology and the logical topology.

The physical topology relates to where users, resources and networking equipment are physically located, and what connectivity is required between users and resources and what connectivity technologies and protocols are available.

The logical topology is dictated to a certain degree by the physical topology, but with the use of VLANs and VPNs the network designer is afforded considerable flexibility when designing the logical topology.

When designing the logical topology the network designer will need to take into account the security requirements for users, resources, data and traffic, and try to arrange users and resources with the same security into groups.

When all of the trust zones have been established, the network designer can then develop the network trust model. The trust model will specify which parts of the network are highly trusted, which parts are trusted less and which parts are not trusted at all.

The trust model will also categorize network traffic into types of traffic that are trusted, trusted less and not trusted at all, and what types of traffic - or what types of data in motion - require high levels of protection, less protection or no protection at all.

The trust model will also help to determine if previously defined network work groups happen to align with trust zones, and if multiple work groups should be logically grouped into the same trust zone, and if there are users, devices and work groups that should be logically separated from others.

When defining a trust zone it may be necessary to also define allowed access between users and services in different zones. Such limitations may involve use of firewalls, or simply ACL in routers.

Network trust zones will be delimited by ACLs in routers or next generation firewalls and are controlled and/or monitored by a network security device. A trust zone may include private IP addresses, whole or partial subnets, VLANs and VPNs.

Recommendation: the network designer should determine how many trust zones are required, define the trust zones and document the trust zones using a network trust model.

How do Trust Zones help with Security?

By themselves, trust zones contribute nothing to network security. The juncture between trust zones must be monitored and/or protected with security tools, otherwise the reason for creating trust zones is defeated.

The juncture between trust zones can be monitored or protected with many different types of security tools acting alone or in conjunction with each other. Some of the security tools available to the network designer are; IDS solutions, IDPS solutions, Next Generation Firewalls, L2 and L3 devices with integral Access Control Lists and Network Access Controllers. More information on the available security tools can be found in later chapters of this document.

In conclusion: properly segmenting the network into trust zones protects sensitive traffic and resources, and furthermore the use of trust zones reduces the scope of any security compromise and buys the administrator time to respond to it.

Access and Distribution Layer Security

From a security perspective, the network Access layer is possibly the most vulnerable layer of the network, this is where users connect their network devices and IP phones to the network.

Companies have historically relied on physical security and employee authorization procedures to secure the Access layer. However in most environments there are non-employees such as contractors, guests and suppliers present in areas where connections to the Access layer are located.

Once a guest or contractor is inside the organization's premises, it is relatively simple for them to connect their computer to an ethernet connection and gain access to the network, conference rooms and lobbies often provide accessible network connections. To compound this problem, the proliferation of Wi-Fi networks and Wi-Fi enabled mobile devices has created a situation where network access may be gained without making a physical connection.

The potential threats from non-employees increases dramatically in cases where organizations provide network services to the public, such as; the hospitality, educational and medical sectors.

Another trend over the past several years that has increased the potential for network threats is the introduction of company policies that allow employees to bring their own devices (BYOD) onto the organization's premises.

The Distribution layer is used to connect the Access layer to devices located in the network Core, the Distribution layer also connects devices connected at the Access layer to each other.

Due to its location in the network hierarchy, the network equipment located in the Distribution layer forms the next layer of defense for assets located in the Core from attacks originating at the Access layer.

The Distribution layer is primarily constructed with L2 switching equipment and some L3 equipment, which means that many of the security tools used to protect the Access layer are also applicable to protecting the Distribution layer.

Access Layer Security Requirements

The Access layer needs to satisfy the following security requirements:

- Access control mechanisms must be available
- Network services need to be available for authorized users
- Some network services may need to be provided to guests or visitors
- Unauthorized users must be denied access so that intrusions, vandalism, data access and fraud can be prevented
- Network administrators and System Logging servers need to be notified of unauthorized access attempts
- A balance needs to be struck between ease of access for authorized users and complexity of the security measures
- Network infrastructure and end points must be protected
- Confidentiality of data and data integrity must be ensured

Access Layer Security Threats

There are several types of threats that can be directed at the Access layer, the more common threats are:

- Denial of Service attacks (DoS)
- Unauthorized access to network resources
- Data theft and data modification
- VLAN hopping
- MAC attacks
- DHCP attacks
- ARP attacks
- Spoofing attacks

Access Layer Security Measures - Recommendations

There are many tools and techniques that can be employed to secure the Access layer; this section provides the designer and administrator with recommendations for securing the Access layer.

Physical Port Security

Physical port security is the first line of defence at the Access layer. Loose network cables should not be left lying around in work areas, conference rooms or lobbies - a loose network cable is an open invitation for someone to connect to the network.

Unused wall jacks are an opportune place for uninvited guests to connect, if the wall jack is truly unused, the administrator should disable the wall jack at the Access L2 switch.

If unused wall jacks are intended for guest connections, then they should be connected to a guest or visitor VLAN, with appropriate access restrictions.

L2 Access switch port, controlling access

To control access to the network, the system administrator should make use of a port based network access control protocol such as IEEE 802.1X.

L2 switch vendors may also support Ethernet Access Control Lists (ACL). ACLs allow the administrator to apply access control rules on L2 ethernet interfaces. The ACL may be based on MAC source addresses, MAC destination addresses, VLAN identifiers or protocol information contained in the IP header.

L2 Switch Advanced Security Features

L2 Switch products offer a multitude of Access layer and Distribution security tools, often these L2 switches also include some L3 networking functions and L3 security features.

L2 switch products typically include; L2 port security, L2 port access control, embedded Intrusion Detection and measures to protect against DoS attacks.

The administrator should ensure that L2 switch security features are configured, activated and, kept up to date.

Wireless network access

Wireless LANs are positioned at the Access layer of a hierarchical network and possesses many of the same vulnerabilities that are found in wired LANs. However, wireless LANs (WLANs) are exposed to additional risks when compared to wired LANs, which means that the network designer must employ additional security measures to guard against unauthorized access via the wireless LAN.

Additional measures must be taken to secure a WLAN because of the nature of radio communications, for instance:

- Gaining access to a wireless LAN does not require physical access to a network switch jack or a network cable; this means that guests and contractors who have been invited into the organization's premises can potentially gain network access without their hosts even being aware.
- It is very difficult to keep the radio waves used in wireless LAN technologies contained within an organization's building, or in the case of multi-dwelling office buildings, contained within an organization's office space. It's possible for an unauthorized individual to eavesdrop on a wireless LAN from outside of the building; from the parking lot, or from out on the street, and in the case of a multi-dwelling office building, from the comfort of their own office - maybe one floor above your organization's offices.

When designing a wireless LAN, the designer should be aware of the following security solutions and purchase products that offer security solutions that are appropriate for their networking requirements:

- Enterprise quality wireless LAN vendors have included extensive Access Control List capabilities within their Wireless Access Point products.
- The wireless security market has responded to customer's needs with Wireless Intrusion Detection Systems (WIDS) and Wireless Intrusion Protection Systems (WIPS).
- Most enterprise quality Wireless Access Point products support advanced encryption capabilities and authentication protocols. Ensure that the most current authentication protocols are supported and that the WAPs are regularly updated.
- There are Network Access Control solutions on the market that are geared towards protecting WLANs, and these systems can ensure that a user's mobile device has up to date virus protection in place before granting the user network access.

Network Access Control Systems

To properly secure the Access layer, the designer will need to include some form of Network Access Control (NAC) capability. NAC systems help the administrator to optimize network accessibility for legitimate users while providing a high level of protection against unauthorized users attempting to access the network.

Most modern L2 switches are available with some embedded NAC capabilities, such as Access Control Lists that can be configured to secure a physical port or a particular VLAN. For further information consult the L2 switch vendor's product literature.

There are numerous stand alone Network Access Control (NAC) products on the market that provide the administrator with a wide range of choices for controlling network access such as time, location, device and type of operating system. These systems can accommodate special access control rules for guests, contractors and BYOD Wi-Fi users.

Access Layer - Intrusion Detection and Protection Systems

The designer should consider employing Intrusion Detection and Protection Systems (IDPS) between the Access layer and the Distribution layer.

In situations where a WLAN is part of the network, the designer should deploy an IDPS that is optimized for WLAN protection.

Further details on these systems can be found in the Mitel technical paper Network Intrusion Detection and Intrusion Prevention Systems.

Distribution Layer Security Measures - Recommendations

In terms of defenses to protect the network Core, the first layer of defense is the Access layer and the second layer of defense is the Distribution layer.

Since the Distribution layer networking equipment is kept in physically secured locations such as wiring closets and/or telecom rooms (and if it is not, it should be), the L2 network ports in the distribution layer are not exposed to the same high level of risk as L2 network ports in the Access layer.

However, even with a reduced level of risk at the Distribution layer network, there is still a possibility of malicious activity and unauthorized access by contractors, service personnel, insider associated threats or (in the case of public areas) the general public. Therefore, it is recommended that network access ports be protected with the same types of measures as recommended for the Access layer and that unused ports be disabled.

The Distribution layer primarily contains L2 switching gear and some L3 equipment, such as routers and firewalls. The Distribution layer network will be segregated into trust zones through the use of firewalls.

The boundaries between trust zones are key areas of the network requiring security measures. It is recommended that IDPS solutions be deployed at trust zone boundaries. The IDPS solutions could be dedicated IDPS solutions, or IDPS solutions that are embedded in Next Generation Firewalls products.

The specific form of IDPS is not important, what is important is having in place mechanisms that can detect a threat and quickly contain the threat to the trust zone where it was found, preventing the threat from propagating throughout the network.

Network Core Security - Recommendations

The network Core usually contains an organization's most critical computing assets and networking infrastructure. The network Core is protected by security devices in both the Access and Distribution layers. However, a properly designed network will ensure that a last ring of defenses is in place to protect the network Core, since an organization's application servers, data bases, storage networks and core network routers reside in the Core.

Core Routers

If the network has been designed in a hierarchical fashion and trust zones have been carefully established at the Distribution layer, then the job of protecting the core router (or routers) is straight forward.

Each trust zone is associated with a set of security policies, this allows the administrator to implement security policies on a, per subnet or per trust zone basis. Access Control Lists (ACLs) on the core routers are created for each subnet or trust zone. The core router will allow traffic into or out of a particular trust zone based on the ACL policies for that trust zone.

It is also necessary to secure the core routers themselves from attacks. Some key methods that should be used are:

- Management access to the core routers should only be allowed over a dedicated management network or management VLAN.
- Access Control Lists, along with authentication servers and user roles should be used on the management ports to block unauthorized access.
- Access to the management port should be protected with strong authentication measures, such as a one-time password server.
- The number of permissible MAC addresses that can access the management port should be limited to one, or to the minimum number required to cover the number of authorized users.

Intrusion Detection and Protection

The use of IDPS solutions within the Core network are highly recommended, this could involve; dedicated systems to monitor network activity, integrated IDPS solutions that are included with the core routers, and host based IDPS solutions to provide protection to individual hosts.

IDPS solutions are discussed in the Mitel technical paper Network Intrusion Detection and Protection Systems.

Protected Zones

The network designer may decide that very critical servers or storage area networks require an additional layer of protection. If this is the case, the designer may consider using a firewall to create a protected zone inside the Core, the critical resources would be located inside this protected zone. The boundary between the core and the protected zone could be monitored with IDPS solutions, or a fully integrated solution such as a Next Generation Firewall (NGFW) or a Secure Access Gateway (SAG).

Security and Management Networks - Recommendations

Accepted network design practices typically divide network connectivity into at least two categories, a network that carries the user's data and a network that is used by the network administrator to manage networking equipment and security tools. This can be accomplished via the use of VLANs or by constructing two discrete networks.

(The reader should be aware that sometimes the network that carries user data may be subdivided further, for instance a network for carrying real time VoIP and Video over IP data and a network for carrying the users TCP I/P traffic.)

The network that carries the user's data is often referred to as the production network or sometimes the data plane; this is the network that provides users with connectivity to their applications and servers.

Networks that carry the network administrator's data are often referred to as management networks or management planes. Some networks may have multiple management planes, for example; a network for managing network infrastructure devices such as routers, firewalls and L2 switches, a network for administering users and a network for managing applications.

The infrastructure management plane may be different from the reseller's network and also independent from each of the customer networks.

There may be other networks, including but not limited to storage networks and infrastructure dedicated networks for example a network dedicated for vMotion.

With the proliferation of network security devices there is a need to provide the administrator with access to the management interfaces on the devices that form the network security infrastructure such as IDPS solutions, NACs and NGFWs.

The network designer may choose to connect to the management interfaces of the network security devices via the network that is used for managing network infrastructure, or the designer may choose to implement a separate management network that is used for communicating with network security devices.

Either way, the point is that the management of the network infrastructure and the management of the network security devices should be performed over one or more networks that are separate from the production network.

From a security perspective, the benefits of having the management network(s) for network infrastructure and security tools segregated from the production network are:

- A dedicated security management network allows very strict access controls to be imposed on management interfaces and makes it very difficult for users connected to the production network to gain access.
- If the production network is subjected to a DoS attack, or if some kind of a storm or flood is in play on the production network:
    - The administrator will still be able to access the management interfaces of the networking equipment and the security tools and restore order.
    - Security tools will be able to communicate with each other and the SIEM so that attack information may be shared, alarms can be sent to the administrator and preventative measures can be communicated to other devices.

- If a networking device has failed on the production network, or a network connection has been severed - the administrator will be able to reach the management interfaces of the networking equipment or security tools, which means that the administrator will be able to troubleshoot the network problem.

Discussions so far have dealt with the design of the network that carries the customer's data - the production network, and focused on the benefits of using a hierarchical network design, and placing networking equipment into the appropriate network layer, Access, Distribution or Core.

While it is often possible for an administrator to gain access to the management interfaces of a router, L2 switch or security device via the production network - most vendors support in-band management interface access, the network designer is advised not to use this method since it would expose this management interface to general users on the production network.

The network designer is advised to use a dedicated network for connecting to the management interfaces of all the networking equipment, such as routers, firewalls and L2 switches. IDPS equipment, SIEMs and other security tools should also be managed over this dedicated network or over a separate security management network. If implementing a completely separate network for managing network devices and security tools is not feasible, then the network designer should consider using VLANs to provide a level of isolation from the production network.

Quite often, network routers and switches will provide the administrator with the capability to configure which interfaces will and will not accept the reception of management packets. If possible, the administrator should make use of this capability to enhance security for the router or switch by blocking unauthorized management access from the production network.

Many devices provide serial interfaces for initial setup as well as CLI access. For a remotely controlled network it is advised to make these interfaces IP accessible on the service provider network.

Chapter 6 Securing the UC Network

Mitel's UC solutions consist of a number of applications that provide services such as IP telephony, unified messaging, audio conferencing and video conferencing. The UC solutions also include management tools, monitoring tools and specialized Session Border Controllers.

Depending on the reference architecture chosen, these applications may be deployed on Mitel proprietary hardware and/or Industry Standard Servers (ISS), or applications may be deployed as virtual applications in a VMware environment.

The Mitel UC solution is overlaid onto a data network, in the case of on-premise architectures, the data network is typically owned by the end customer. In the case of Cloud architectures, the Cloud portion of the network will be owned by the service provider and the on-premise portion will usually be owned by the end customer.

The portion of the underlying data network that is utilized by the UC solutions is referred to as the UC network.

This chapter provides recommendations as to what the network designer should do to ensure that the UC network is secured against attacks and intrusions.

It is important to keep in mind that security recommendations are not provided for the portions of the network that are not involved in supporting the UC solution. However since it is possible for threats to originate from anywhere in the network, It is expected that the network designer will take the appropriate measures to secure the portions of their data network that are separate from the UC network.

UC Solution Assets

From a security perspective, the UC MLB/Private Cloud Solution assets are the components and applications that comprise the UC Solution, UC Solution management and monitoring applications, user data and user media streams.

With the exception of management applications and management tools, the UC MLB and Private Cloud Solutions employ identical assets.

The management solutions for the UC MLB solution and the UC Private Cloud solution differ as follows:

- The UC MLB solution is managed with Oria and MMG.
- The UC Private Cloud solution is managed with Enterprise Manager

The following paragraphs describe the UC Solution assets:

MiVoice Business (MiVB)

MiVoice Business is a software based product that includes the call control engine and integrated media services, MiVB can installed onto an Industry Standard Server (ISS), a server running VMware or onto a Mitel 3300 IP Communication Platform (ICP). The MiVB performs all call processing functions and associated call signaling to IP endpoints.

MiCollab

MiCollab provides the infrastructure that allows for a number of Mitel applications to be grouped together into a Unified Communications solution; MiCollab runs in a VMware virtual environment.

MiCollab supports all forms of collaboration, including voice calling, video calling, and instant messaging with Mitel MiCollab Client, and Web presentation and collaboration with Audio, Web and Video Conferencing (AWC).

MiCollab provides co-residency of the following applications:

- MiCollab Client
- MiCollab Audio, Web, and Video Conferencing
- MiVoice Border Gateway
- MiCollab Unified Messaging, this is a UC voice mail application that includes various messaging options

MiCollab also integrates with and provides enhanced communications and collaboration functionality to business applications, including Microsoft Outlook, Google Mail and IBM Lotus Notes.

MiVoice Border Gateway Virtual (MiVBG)

MiVBG is also a specialized application proxy supporting SIP, MiNet, and a number of web protocols; the application is deployed on a server running VMware or onto an Industry Standard Server.

Some of the key functionality provided by the MiVBG includes:

- Teleworker service for connection to remote SIP and MiNet end-points
- SBC functions and SIP trunk proxy for connection to external third-party SIP providers
- Web proxy for externally connected devices such as: MiCollab mobile clients and Softphones, management access, and access to LAN-based applications.

Mitel Open Integration Gateway (OIG)

The Mitel Open Integration Gateway (OIG) provides a proxy for connections to Customer Relationship Management (CRM) business applications, and IT applications. OIG also provides API connectivity for 3rd party applications.

Oria & MiCloud Management Gateway

Oria is Mitel's solution for managing Mitel's UC Cloud solutions. Oria is deployed on a server in the data centre and is the primary management tool for service providers, resellers, customers, and end-users to access and modify services.

Oria is deployed as part of the reseller or service provider management network and is not deployed per customer. The access to the customer network is via the MiCloud Management Gateway.

Oria offers the following capabilities:

- **Access control:** Oria can be used to define unique profiles for users, limiting access to sensitive information, and provide personnel with the features they need to execute their responsibilities effectively, including controlling what a Customer Administrator can see or do. Access control can be set up for service provider administrators, resellers and customer administrators.
- **Operations integration:** Oria can be integrated into any Service Provider's operational systems.
  - Oria includes an API allowing for integration with order entry systems
  - Oria can generate reports which can be used by billing systems

The MiCloud Management Gateway, (MMG) provides a service provider with the ability to manage multiple customer sites from one Oria.

The MMG has two network interfaces. The first network interface is connected to the management network and the second network interface is connected to all the customer networks via a VLAN trunk. Each customer network must be on a unique VLAN.

Note: Oria and MMG are only used with the UC MLB solution.

Enterprise Manager

Enterprise Manager is a centralized management application providing access from a single interface to multiple systems within the customer’s network, use of Enterprise Manager is optional.

Note: Enterprise Manager is only used with the UC Private Cloud solution.

Native Management Interfaces

These are direct management interfaces to the individual products, including:

- Individual applications
- Network and virtualization infrastructure
- Call control engines

MarWatch Server and MarProbe

MarWatch is an application that manages and monitors the UC solution and the associated network infrastructure on a 24/7 basis. MarWatch offers secure remote access for troubleshooting, and MarWatch also provides real-time alerts when potential network issues are detected.

The MarWatch application uses a virtual probe called the MarProbe to collect fault and performance data from Mitel UC components and selected network devices. The MarProbe is deployed in the actual network to be monitored, and transfers the data that it has collected to the MarWatch server. When the MarWatch server is not located in the same network as the MarProbe, the MarProbe will communicate with the MarWatch server via an internet connection.

vSphere Client & vCenter

The vSphere client is used by the service provider to manage individual VMware servers. vCenter is used by the service provider to manage the overall VMware environment.

Business applications

These are customer specific business applications that the UC system may need to be aware of, or to integrate with such as:

- Email
- Business applications
- IT applications

Teleworker (Public Network)

This network provides connectivity for Teleworker clients. This access is typically over a Public Internet connection, or over a publicly-accessible network. This network uses the MiVBG to provide public internet to private internal address translation for a single customer.

SIP Trunk Provider

The SIP trunk provider offers customers SIP trunk connectivity, the offering includes:

- DDI/DID numbers that are hosted or assigned by the SIP service provider
- SIP to PSTN access
- IP Network isolation via an SBC
- Billing
- E911 location information

PSTN

The term Public Switched Telephone Network (PSTN) describes the various equipment and interconnecting facilities that provide analog and TDM phone services to the public.

UC Solution Network Security Models

This section includes descriptions and drawings of network security models for the UC MLB solution and the UC Private Cloud solution. The network security model diagrams identify the trust zones for each UC solution, and identify the junctions between trust zones that require security controls.

The network security model diagrams are generic; the network designer may need to modify the models to accommodate the individuality of their own network.

Some networks will be simpler and other networks will be more complex than what is shown in the network security model diagrams. For example, some customer sites may have only IP phones and a basic access network located on premise; other customer sites may have extensive on premise networks, providing connectivity to several applications located on premise.

Some customer sites may require additional trust zones - beyond what is shown in the security model diagrams, for instance a particular site may have requirements to provide different network access controls for guests and visitors than the access controls provided for employees, such a situation would warrant the creation of a trust zone strictly for guests and visitors.

The network designer will need to review the recommended security model and consider the details of their own network before finalizing their own security model, but the basic principles illustrated - identifying the trust zones and deploying security controls between trust zones remains valid for all sizes and complexities of UC solutions.

Security Model Drawing Conventions

The Security Model diagrams (Figures 3, 4, 5 and 6) adhere to the following drawing conventions:

Colours: Colours are used to indicate the security risk associated with a particular trust zone. Network segments, WAN connections, Clouds and networking equipment are coloured according to the trust zone that they are included in or associated with.

Untrusted Zones

- **Red:** Red is used to denote an *untrusted* zone. In the UC Trust Models, the internet is considered to be *untrusted.*

  If a particular customer site had a requirement to provide network Access to the public or to their guests, it would be appropriate to designate this Access network as *untrusted*. For example, if a coffee shop, hotel or cruise ship is providing the public with network Access, then this network should be designated as *untrusted*.

  Similarly, Access networks for students in schools and university dormitories or Access networks for patients and visitors in a health care facility should be designated as *untrusted*.

Semitrusted Zones

- **Orange:** Orange is used to denote a *semitrusted* zone that is used for SIP trunk access and PSTN access. PSTN and SIP service provider communications are considered to be part of a *semitrusted* trust zone because of the nature of the media involved and the fact that the service providers will have their own security measures in place.
- **Brown:** Brown is used to denote a *semitrusted* zone that is used to access business applications. Because the business application providers provide their own access control and security measures, this network is considered *semitrusted*.

Trusted Zones

- **Green:** Green is used to denote a *trusted* zone that is used to provide connectivity for UC voice, UC data and management of UC applications. The UC voice and data network is designated as *trusted* because the appropriate security measures are in place at all network access points and at all of the junctures where the UC voice and data network interfaces to less trusted trust zones.
- **Purple:** Purple is used to denote a *trusted* zone that is used for accessing management interfaces on network switches, routers, and network security devices. The security management network is designated as *trusted* because the appropriate security measures are in place at all network access points and network junctions with less trusted zones.

- **Blue:** Blue is used to denote a *trusted* zone that is used to provide UC management access from the Service Provider and the Management networks to the voice and data network. Because both the Service Provider and the Management sites provide their own access control and security measures, this network is considered *trusted*.

Symbols and Acronyms: The symbols and acronyms that are used in the network security model diagrams are described below:

- **Next Generation Firewall (NGFW):** These devices are depicted with the standard 'router' symbol. NGFWs usually have integrated IDPS capabilities. The type of IDPS and the degree of protection need to be decided when selecting the NGFW to be deployed at a particular junction.
- **Network Access Control (NAC):** Blue and white shields indicate the locations where NAC capabilities are deployed. NAC capabilities are included in many L2 switches and routers, NAC solutions are also available as standalone products. The sophistication of the NAC selected for use at a particular network location will depend on the level of control the designer feels is justified.
- **Web Application Firewall (WAF):** Standalone Web Application Firewalls are depicted with a grey box; WAFs that are integrated into NGFWs are indicated with a text label.
- **Grey Shields:** Grey shields are also used to indicate that a particular component or application is a security device.

UC MLB Security Model

The UC MLB security model is depicted in Figures 3 and 4, Figure 3 shows the cloud portion of the network and Figure 4 shows the customer premise portion of the network. A description of the model is provided following Figure 6.

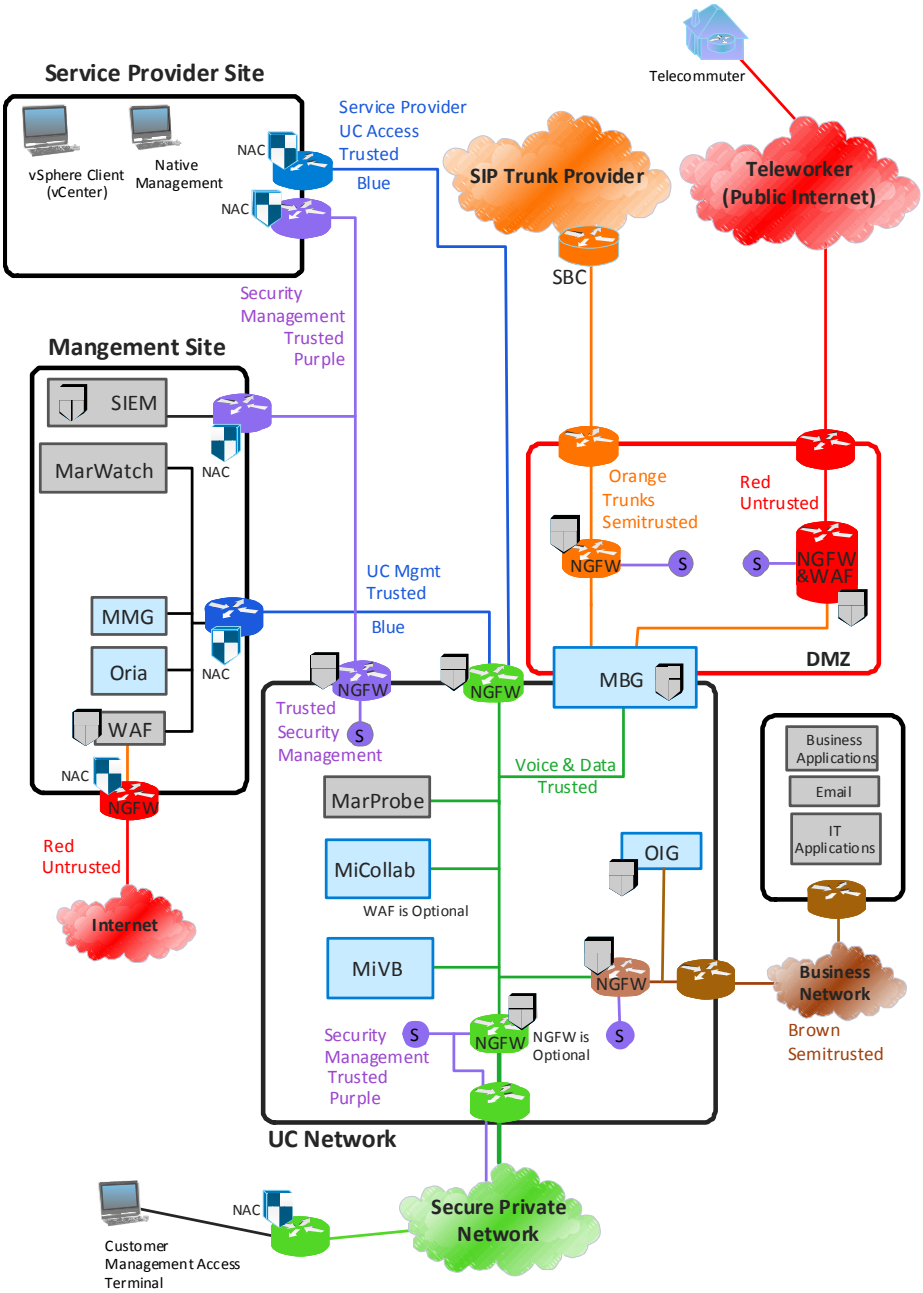

Figure 3 Security Model for Cloud Portion of UC MLB Solution

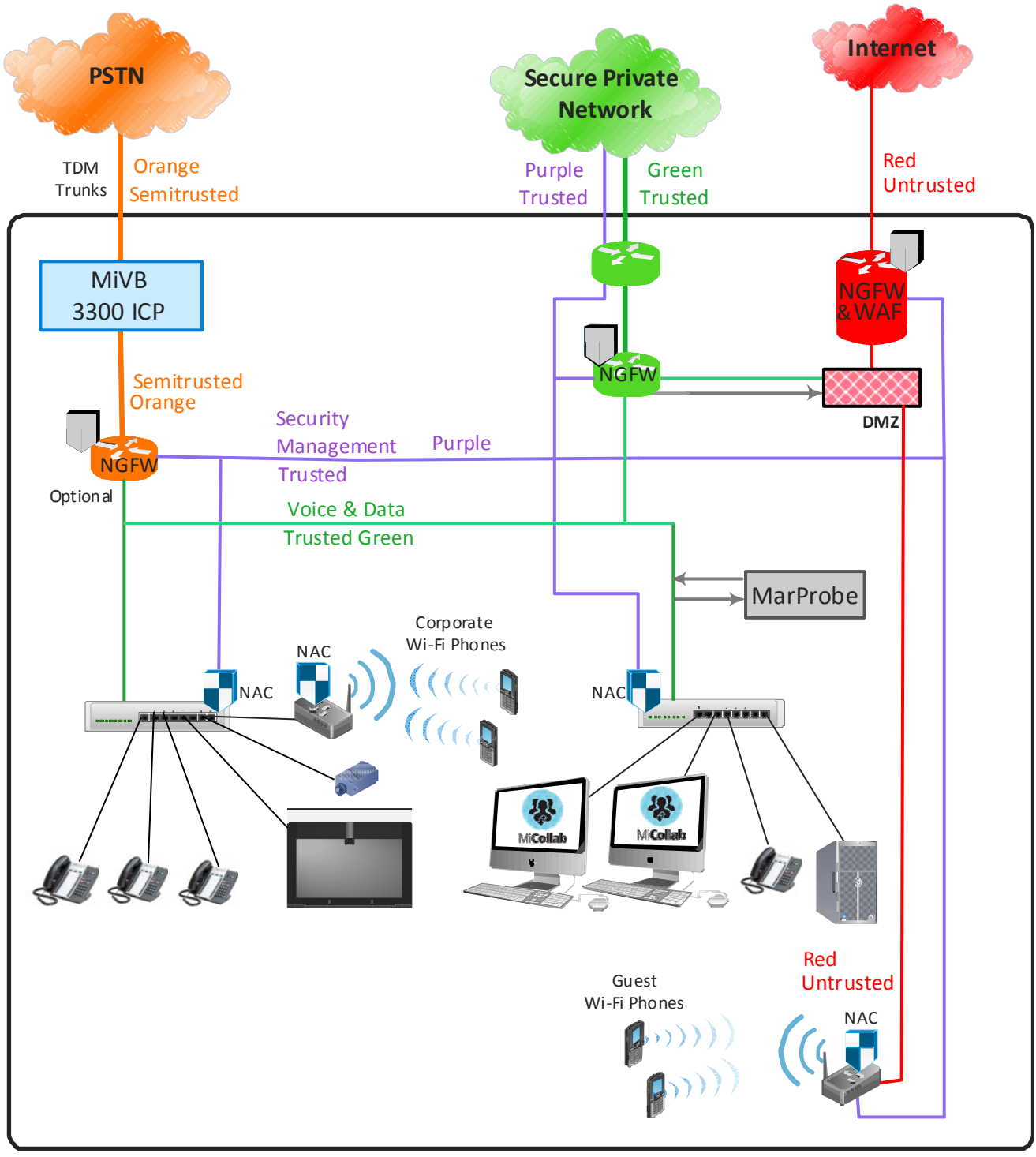

Figure 4 Security Model for On Premise Portion of UC MLB Solution

UC Private Cloud Security Model

The UC Private Cloud security model is depicted in Figures 5 and 6, Figure 5 shows the cloud portion of the network and Figure 6 shows the customer premise portion of the network. A description of the model is provided in Figure 6.

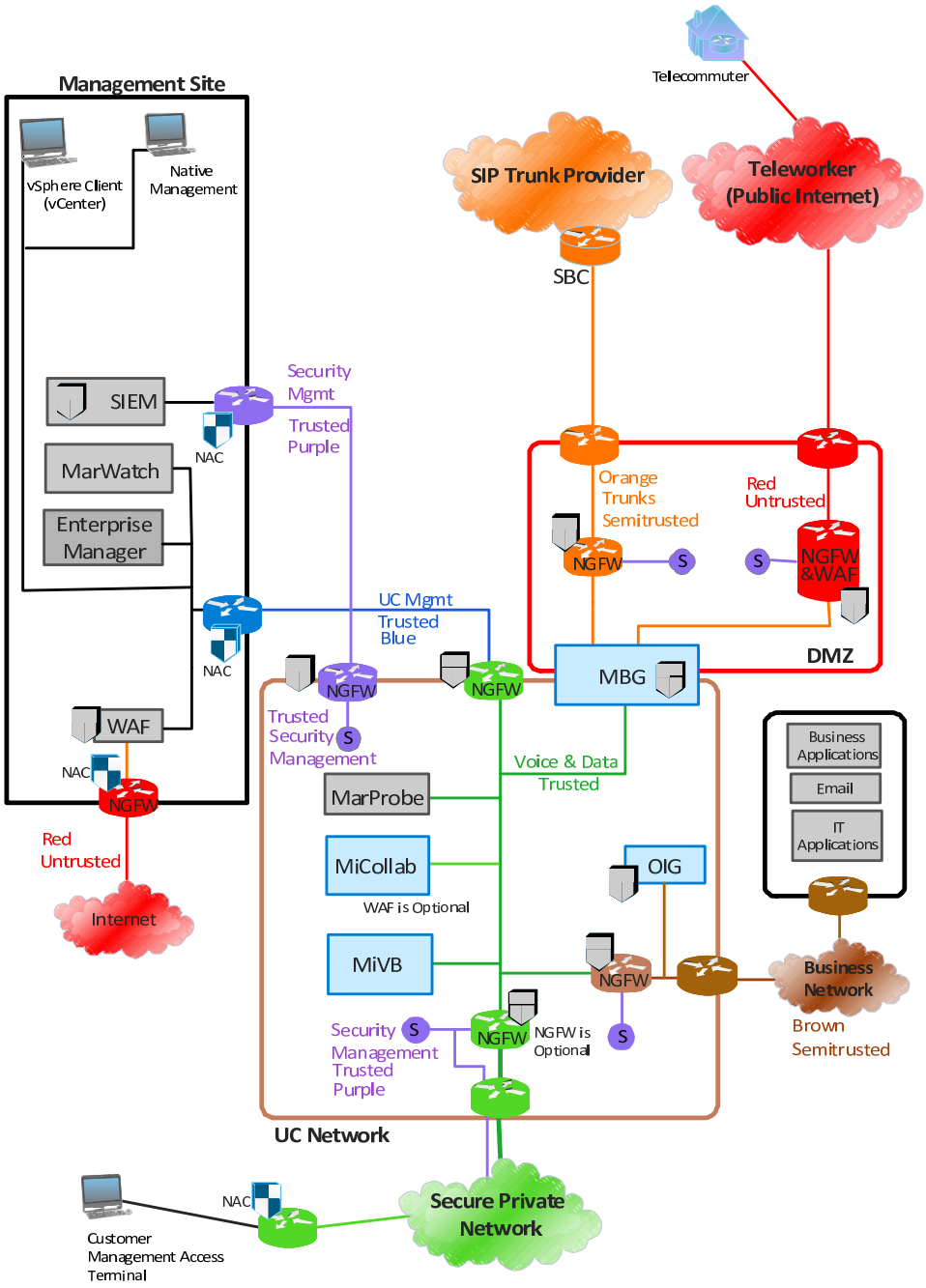

Figure 5 Security Model for Cloud Portion of UC Private Cloud Solution

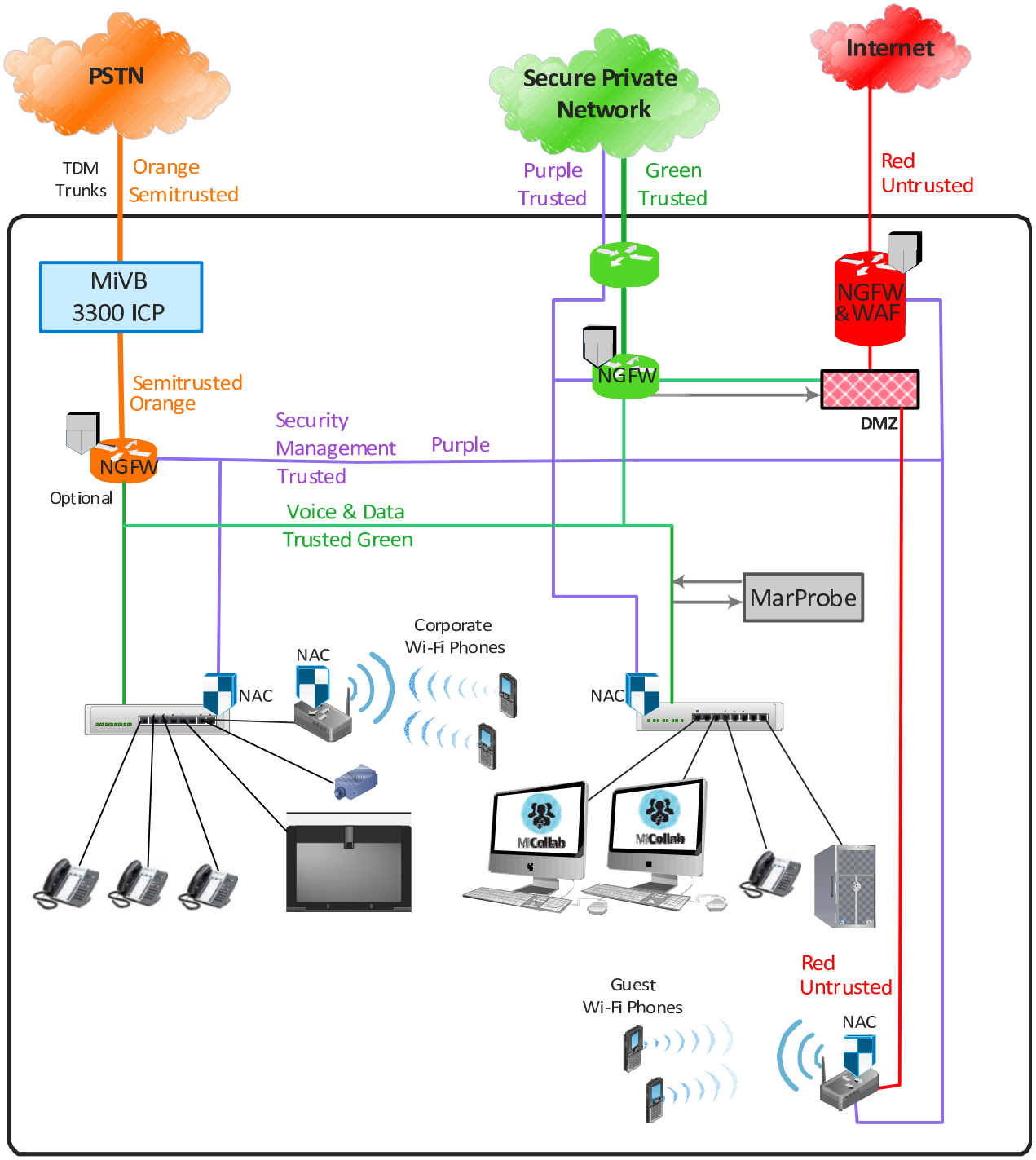

Figure 6 Security Model for On Premise Portion of the UC Private Cloud Solution

Security Model Descriptions

This section describes the UC MLB and the UC Private Cloud Security Models. The descriptions provided are applicable to both MLB and Private Cloud Security Models. The reader should reference Figures 3 through 6 when reviewing these descriptions.

Trust Zones

The UC security model is based on partitioning the network into various trust zones, and deploying the appropriate security measures at the network junctions between the different trust zones. There are trusted zones, semi trusted zones and untrusted zones. The next sections provide detailed descriptions of these trust zones.

The Trusted Zones

The UC security model has three networks or zones that are designated as trusted, they are:

- The Voice and Data network, this network carries UC user data and UC management data.
  - UC user data includes real-time voice and video media and associated signaling, and all end user data communications.
  - UC management data refers to the traffic between the system administrator and the management interfaces for UC applications.
- The Security Management network carries management traffic for network security devices/applications and networking equipment such as switches and routers.
- The UC Management network, this network is used to access the management interfaces of the UC products and applications.
  - The UC MLB solution has two UC Management Networks, the Service Provider UC Access network and the UC Management network.
  - The Private Cloud has one UC Management network.

Note: The UC security model uses one network to provide connectivity to the management interfaces of both networking equipment and security equipment; however, the network designer may decide to create two separate networks or zones, one for networking equipment and one for security equipment.

The Voice and Data Network

In the security model drawings, green is used to depict the voice and data network/zone. This trust zone is used to provide connectivity between voice and video UC applications and IP end points.

The voice and data network extends from the customer site (or on premise portion of the network) via a secure private network (i.e. MPLS, Metro Ethernet or VPN network) into the Cloud portion of the network, creating a trust zone that spans multiple geographic locations. The ability to extend this trust zone across the secure private network is accomplished with the use of VLANs, VPNs and Ethernet over MPLS (EoMPLS) technology.

When designing networks for real time data such as voice calls or video conferences, it is important that the security measures deployed in the data path do not adversely affect the media transmission times by contributing excessive network delays.

Real time data is sensitive to network delays and can suffer degradation if network delays are excessive. By keeping all real time traffic in a trusted zone, the network designer has no need to deploy security controls in the data path that introduce excessive network latency due to deep packet inspections and/or protocol analysis.

The Security Management Network

In the security model drawings, purple is used to depict the network that is used for managing network security devices, and networking equipment.

This trust zone is used to provide connectivity between security tools, networking equipment management interfaces and the administrator.

The security management network extends from the customer site (or on premise portion of the network) via a secure private network into the Cloud portion of the network, and then extends further into the management and/or reseller network to reach the SIEM, creating a trust zone that spans multiple geographic locations.

The UC Management Network(s)

For the UC MLB: components and network segments that are in the Service Provider UC Access and Service Provider UC Management networks are coloured blue.

This trust zone is used to provide connectivity from the MLB Service Provider and the MLB Management Sites to the voice and data network.

- The MLB Service Provider site contains the vSphere client for managing the VMware infrastructure and Native management stations for direct management of applications. Access from within this site is controlled by a router and a Network Access Control application, access into voice and data network is controlled with a NGFW.
- The Management site contains the MarWatch and Oria servers. Access from within this site is controlled by a router and a Network Access Control application, access into voice and data network is controlled with a NGFW.

For the Private Cloud: components and network segments that are in the UC Management networks are coloured blue. This trust zone is used to provide connectivity from the Private Cloud Management site to the voice and data network.

- The Private Cloud Management site contains the vSphere client for managing the VMware infrastructure, Native management stations for direct management of applications, the MarWatch server and the Enterprise Manager server. Access from within this site is controlled by a router and a Network Access Control application, access into voice and data network is controlled with a NGFW.

Customers may also be able to access Oria and some native management interfaces from remote locations by connecting over the secure private network.

The Semitrusted Zones

The UC security model has two networks or zones that are designated as semitrusted, they are:

- The Business network, this network is used to access business applications and email systems.
- The Trunk network, this network is used to access PSTN trunks and SIP trunks.

The Business Network

In the security model drawings, brown is used to depict the Business network.

Applications and network segments that are in the business trusted zone are coloured brown. This trust zone is used to provide connectivity from users and applications to business applications. Because the business application providers provide their own access control and security measures, this network is considered semitrusted.

The Trunk Networks

Components, applications and network segments that are in the trunk networks are coloured orange. This trust zone is used to provide connectivity to the SIP trunk service provider and also to the PSTN. Security measures are placed between the semitrusted zone and the trusted zone:

- At the customer site, an optional NGFW with IDPS capabilities may be deployed between the trusted network and the local 3300 ICP that is providing local PSTN breakout. Some network designers may decide that deploying a NGFW with IDPS capabilities at this location is not required since PSTN TDM connections are inherently secure and the 3300 ICP will not grant network access to an intruder attempting to access the network by using a modem over the PSTN connection.
- At the cloud site, a NGFW with IDPS capabilities is deployed in the network DMZ and connects to the SIP trunk provider via a router, the SIP trunk provider will also have an SBC deployed at the edge of their network. Access between the DMZ and the trusted zone is controlled by the MBG.

Note: In addition to the protection provided by the MBG, the designer may wish to provide additional protection against potential attacks coming from the SIP service provider's site. To do so, the network designer may want to consider using a NGFW that is SIP aware and capable of detecting telephony based DoS attacks.

The Untrusted Zone

Components and network segments that are in the untrusted zone are coloured red. This trust zone is used to provide connectivity to the internet service provider.

Security measures are placed between the semitrusted zone and the trusted zone:

- At the customer site, a NGFW with IDPS capabilities is deployed between the trusted network and the local network DMZ. A NGFW with an integral WAF is deployed in the local DMZ and is used to secure access between the DMZ and the internet.
- At the customer site, guests or the public are able to access the internet via a guest/public Wi-Fi network. The Wi-Fi access point connects to the internet through the DMZ.
- At the cloud site, an MBG is deployed between the trusted zone and the DMZ. A NGFW is deployed in the DMZ; this NGFW has integrated IDPS capabilities and an integral WAF. The NGFW connects to a router that in turn connects to the internet service provider.

Network Sites

The UC solution and the management infrastructure are deployed across multiple sites, some sites are in geographically different locations and some sites may be co-located. The following sections describe the security model details for each site involved with delivering the UC solution.

The Customer Site

At the customer site, authorized users access the trusted voice and data network via Access L2 switches. Within the customer's premises, these switches provide the first line of defence and must include DoS protection, some level of IDPS and sophisticated NAC capabilities. If a L2 switch is deployed that does not include NAC, then a dedicated NAC solution that meets the access requirements must be deployed.

Wi-Fi client network access for authorized employees is controlled by ACLs within the Wi-Fi access point, the access points used must be carefully selected to ensure that they have appropriate security controls; additional protection is provided by the Access L2 switch that connects the access point to the copper network.

Wi-Fi client network access for guests and/or the public is controlled by ACLs within the guest Wi-Fi access point. The guest Wi-Fi access point connects via an untrusted network to the DMZ, which in turn connects to the internet.

The MarProbe is installed on the customer site voice and data network and performs passive monitoring of this network. The MarProbe accesses the internet through the customer site DMZ, and communicates with the MarWatch server over an untrusted internet connection.

Note: The administrator may want to ensure that the MarWatch server and the MarProbes use static IP addresses so that the programming of routers can be tightly controlled.

Local PSTN break out is provided by a 3300 ICP running MiVB, the 3300 ICP is installed in a semitrusted zone and access to this semitrusted zone from the trusted zone is controlled by a NGFW with an integrated IDPS solution.

A dedicated network or VLAN is used for communication between security devices and the SIEM; this network forms a trusted zone and is colored purple.

As mentioned previously, some customer sites may need to have additional trust zones established. Certain customers may require that a trust zone be created for the public, guests, students or patients. In these cases, the same principles described here and shown in the security model diagrams can be extended to accommodate the customer's additional trust zone requirements.

The Cloud Site

At the cloud site, MiVB, MiCollab and MBG are placed in the voice and data trusted zone. The voice and data trusted zone extends from the Cloud network into the customer network via a secure private network connection such as an MPLS connection. Users access the UC solution applications via the voice and data trusted network. The NGFW that connects the UC network to the secure private network is optional.

A NGFW with strong access control capabilities is used to connect the trusted network to the Service Provider's network and the Management or Reseller's network.

A NGFW with access control and IDPS capabilities is used to connect the trusted voice and data network to the semitrusted business applications network, which is coloured brown. The business application providers provide their own access control and security measures, as a result this network is considered semitrusted.

The OIG serves as a proxy between UC applications and business applications and is located in the semitrusted business network.

UC MLB Service Provider Site and Private Cloud Management Site

For the UC MLB Solution: the Service Provider site houses clients that are used to access the native management interfaces on the UC applications, clients that are used to access the native management interfaces on network routers and switches and clients that are used to access VMware infrastructure.

The Service Provider's site should employ a router with access control capabilities or a separate NAC to provide:

- vSphere with access to the voice and data network.
- UC application native management clients with access to the voice and data network.
- Network switch and router native management clients with access to security management network.

For the UC Private Cloud Solution: the clients described above are located within the Management Site.

UC MLB Management Site and Private Cloud Management Site

The UC MLB Management Site houses the Security Information and Event manager (SIEM), the MarWatch server and Oria.

The Management Site should employ a router with access control capabilities or a separate NAC to provide:

- MarWatch and Oria with access to the voice and data network.
- The SIEM with access to the security management network

The SIEM, MarWatch and Oria support browser based user interfaces; these interfaces are intended to be accessed by the administrator over an internet connection. Security between this network and the Internet is provided by a NGFW with NAC and a WAF.

For the UC Private Cloud Solution: with the exception of Oria and MMG, the applications and severs described above and Enterprise Manager are located within the company's Management Site.

Chapter 7 Unifying Next-Generation Security Tools

This document has provided the network designer with recommendations on deploying several network security measures such as IDS, IDPS, NGFWs, advanced Layer Two Switches, NAC measures, Wi-Fi NAC measures and Host based IDPS.

Based on these recommendations it would seem that from a network security perspective all the bases have been covered, but to have a truly effective security solution all of the security devices need to be unified by a centralized security management solution.

The application that is typically used to provide this centralized management function is a Security Information and Event Manger (SIEM). However some security device vendors may provide a separate security management solution that is intended to work in conjunction with a SIEM.

Whether a network is designed with just a SIEM or with a proprietary management application and a SIEM will depend on which security solution the network designer chooses to purchase. Which of these two management approaches are used is not important, what is important is that a management solution is put in place that allows for the unification of reporting, managing and monitoring.

The security management solution should be able to manage and monitor all portions of the UC network, both Cloud and on premise based components.

The network designer will also need to decide if the UC network security management tool should communicate with the IaaS or PaaS provider's security management SIEM and components. Whatever is decided should be carefully described in the SLA or contract between all the involved parties.

There are government and industry sponsored initiatives in place that are intended to foster interoperability between different vendor's products. Both the NIST and the U.S. Department of Homeland Security have published recommendations, specifications and test methodologies to encourage security device interoperability. The network designer may find these publications to be useful when investigating interoperability of security devices and management systems.

A security solution that is unified under a single management system will allow security personnel to be more productive and allow for reduced response times to a network attack.

Security Information and Event Management

A Security Information and Event Management system (SIEM) is a product that combines the security information management system (SIM) and the security event management system (SEM) into one solution.

SIEMs are available as software products that run on a customer supplied industry standard server, as a turnkey appliance or as a managed service.

The SIEM provides the administrator with the ability to view data from all of the network security devices in a single place. This centralized view makes it easier to detect and analyze network trends and patterns that are out of the ordinary, and recover from security events.

Most SIEMs will collect event data from the security devices using standards based logging protocols or SNMP. It is important that the network designer ensure that the security tools being considered for deployment employ a common communications protocol - standards based protocols are preferred over proprietary protocols.

Dedicated Management Networks for Security Tools

Organizations should consider using a dedicated security management network for connecting security devices to each other, the SIEM and if required a management application.

The benefits of having a dedicated security management network for interconnecting security tools and the SIEM are:

- A dedicated security management network allows very strict access controls to be imposed on management interfaces and makes it very difficult for general users that are connected to the production network to gain access.
- If the production network is subjected to a DoS attack, or if some kind of a storm or flood is in play on the production network:
    - The administrator will still be able to access the management interfaces of the security tools and restore order.
    - Security tools will be able to communicate with each other and the SIEM so that attack information may be shared, alarms can be sent to the administrator and preventative measures can be communicated to other devices.
- If a networking device has failed on the production network, or a network connection has been severed - the administrator will still be able to reach the management interfaces of the security tools.

Dedicated security management networks are covered in more detail under Network Architecture.

Conclusion

The key to ensuring that the network security solution is truly unified is to select security products and applications that can interoperate seamlessly with each other.

Each security tool, be it an IDPS, a NGFW or an access control device, will have its own strengths and weaknesses.

When all of the individual security solutions are able to share information the overall security solution will be more effective since it will benefit from the individual strengths of each security solution.

While the individual security tools are able to operate independently if they have to, when all the components from the access layer to the core work in concert with each other the end result will be a defense-in-depth strategy that is able to deal with attacks originating at any layer of the network, from edge to core.