



Apptix Business Messaging & Collaboration – Information Security

A White Paper



Table of Contents

1	EXECUTIVE OVERVIEW	2
2	STANDARDS & POLICIES	3
3	PEOPLE	4
4	PHYSICAL SECURITY	4
5	ADMINISTRATIVE SECURITY	4
5.1	INCIDENT RESPONSE PROCEDURES.....	4
5.2	SEPARATION OF DEVELOPMENT AND OPERATIONAL FACILITIES	4
6	RELATIONSHIPS	4
7	TECHNICAL SECURITY MEASURES	4
7.1	NETWORK SECURITY	4
7.1.1	<i>Message Encryption.....</i>	4
7.1.2	<i>Perimeter Security</i>	4
7.1.3	<i>Denial of Service (DoS) Attacks</i>	4
7.1.4	<i>Spam Prevention.....</i>	4
7.2	HOST & APPLICATION SECURITY	4
7.2.1	<i>Server Security.....</i>	4
7.2.2	<i>Malicious Software Security.....</i>	4
7.2.3	<i>Multi-Tenancy.....</i>	4
7.3	SECURE ACCESS CAPABILITIES	4
7.3.1	<i>MAPI Connectivity.....</i>	4
7.3.2	<i>Outlook Web Access (OWA)</i>	4
7.3.3	<i>AdminCenter & UserCenter</i>	4

1 Executive Overview

Achieving information security requires more than just technical solutions, although that's where the attention seems to focus. We have developed a robust multi-faceted security program, going beyond black boxes and software.

Naturally, we have technical security solutions in place. Our networks are protected by best-of-breed Cisco firewalls. Our team of network engineers tightly secures and maintains all network components. Virtual Local Area Networks (VLANs) isolate service elements from each other and the outside world. Virtual Private Networks, frame relay and dedicated lines are used where appropriate to security network connections. Our Trend Micro anti-virus solution is top-notch. Operating systems and applications are "locked down", using automated tools, developed in-house, to, ensure that unnecessary services are turned off and tight security settings are in place.

Our systems are hosted in world-class Data Centers. These state-of-the-art facilities boast the finest physical security in the industry. Housed in unmarked buildings, entrance to these facilities is extremely limited and is protected on a 24x7 basis by technical and human sensors. Security guards are at every corner, video cameras watch over all activities, and a comprehensive network monitoring system is in place. Locked cages separate our equipment from that of other companies. Electrical power is redundant, as is network access. The data center's environment is tightly controlled. These facilities are engineered to protect information assets from natural disasters such as fire and earthquakes.

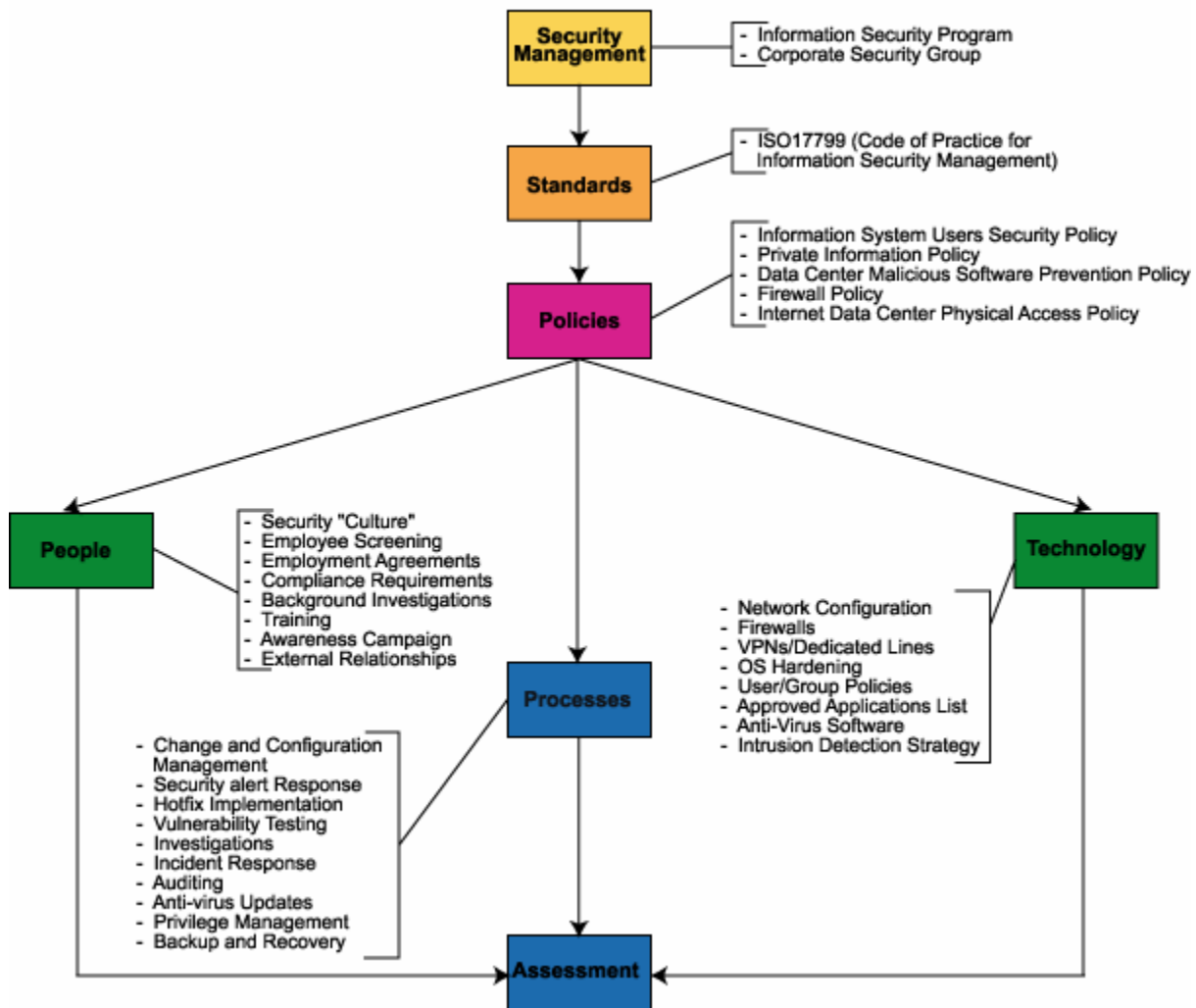
But beyond these technical solutions, we have a security plan and a security program. With the commitment of top-level management, we have put in place a strong global security organization using international standards to guide policy development from which crucial security processes are identified. This program combined with the very best technology available today and with awareness that people are our greatest security tool, minimizes the security risk our customers face.

The cornerstone of a successful information security effort is commitment from the highest levels of management. This commitment is manifested not only by the devotion of resources, but by the example these executives set. The commitment to security starts with the Chief Executive Officer, who, in conjunction with the Chief Technology Officer, implements the Security Management Program. This program designates and incorporates security responsibilities, program goals and objectives, as well as the organizational structure necessary for successful accomplishment of our worldwide information security objectives.

2 Standards & Policies

Serving as a guidepost for the overall security program is the International Standards Organization's Code of Practice for Information Security Management (ISO17799). Standards exist as a means by which an organization can better ensure that its policies, procedures, and tools are in consonance with the best practices in existence. While there is no single accepted standard for managing information security programs, ISO17799 enjoys widespread credibility. ISO17799 is based on a British Standard (BS7799), which is a national standard in some countries, the standard for many well-known corporations and organizations, and is widely used throughout the world. By adopting ISO17799 as the standard for information security management, the International Standards Organization (easily the best known and most respected international standard-setting organization) bestows credibility on the merits and recognition of the standard.

Policies are the roadmaps that we use to make sure that our security program is heading in the right direction. Security policies cover the gamut of security issues. Physical security, information privacy, information system users, operations, and development are all security areas that are covered by current or planned policy. All policies meet or exceed the requirements of ISO17799. The figure below depicts the relationship between the overall security program, standards, policies, processes, technologies, people, and assurance.



3 People

Your information is only as secure as the people who handle it. Recognizing this fact, personnel security is developed beginning the day an employee is hired. All job descriptions include the security responsibilities that the employee will be expected to understand and meet. Potential employees undergo background investigations that may include identity, criminal and credit checks, former employer reference checks, and education verification. Employees vying for more sensitive positions, such as data center operations, undergo more rigorous checks. To further ensure we have the best people in the business, we require our engineers to be trained and certified, and we have programs to help them meet these requirements. Our procedures help ensure that only those professionals with the best abilities, trustworthiness and integrity are employed. Because security is such an important facet of our business, we stress security awareness. We are developing a security culture, emphasizing security to our team at every turn.

4 Physical Security

Access to production facilities is granted only to those engineers who specifically require that access in order to conduct their duties. The majority of this work takes place remotely, requiring rare physical access to the production facilities. Housed in unmarked buildings, entrance to these facilities is extremely limited and is protected 24x7 by technical and human sensors. These facilities have the following physical security features:

- Motion sensors.
- Video camera surveillance.
- Security breach alarms.
- Biometric access control.
- HVAC temperature control systems with separate cooling zones
- Seismically braced racks.
- State-of-the-art smoke detection and fire suppression systems.
- Redundant Power Distribution systems with Battery and Generator backups

5 Administrative Security

One of the most powerful security tools available is a trained, proactive, knowledgeable system administrator who is acutely familiar with her system. Data centers are manned by experienced engineers. Our system engineers closely monitor our systems to assure that any potential security issue is addressed quickly and completely. Security alerts are monitored and screened for applicability to production systems. HotFixes and service packs are applied as needed. Emerging virus threats garner particularly close attention so that we always have the most up-to-date anti-virus software solutions available. Security Engineers conduct random penetration testing and generate reports of potential issues. Like all security issues, these reports get immediate attention. Our operations teams, using policy as a guide, develop systematic, repeatable procedures covering a broad spectrum of data center activities, including daily administration, audit log review, data backup, antivirus updates, and configuration management.

5.1 Incident Response Procedures

Equally important to the technical security measures are detailed job procedures that instruct operations and support personnel on the tasks they must perform in order to ensure the security of our service and our customer's information. These procedures include periodic (daily, weekly, monthly) security maintenance procedures as well as the detailed incident response procedures that are followed in the event of a *security incident*. Detailed incident management procedures have been established to cover all types of security incidents, including:

- information system failures and loss of service
- denial of service attacks
- malicious software attacks
- breaches of confidentiality

In addition to normal contingency plans (designed to recover systems or services as quickly as possible) these procedures also cover:

- analysis and identification of the cause of the incident
- planning and implementation of remedies to prevent recurrence, if necessary
- collection of audit trails and similar evidence
- communication with those affected by or involved with recovery from the incident
- reporting the action to the appropriate authority

5.2 Separation of development and operational facilities

Separating development, test and operational facilities is important to prevent serious problems (e.g. unwanted modification of service delivery environment causing system failure). Procedures for the transfer of software from development to operational status are well defined, documented, and executed accordingly.

A high degree of separation is maintained between operational, test and development environments in order to prevent these types of operational problems. A similar separation also exists between development and test capabilities, ensuring that a known and stable environment in which to perform meaningful testing is maintained.

6 Relationships

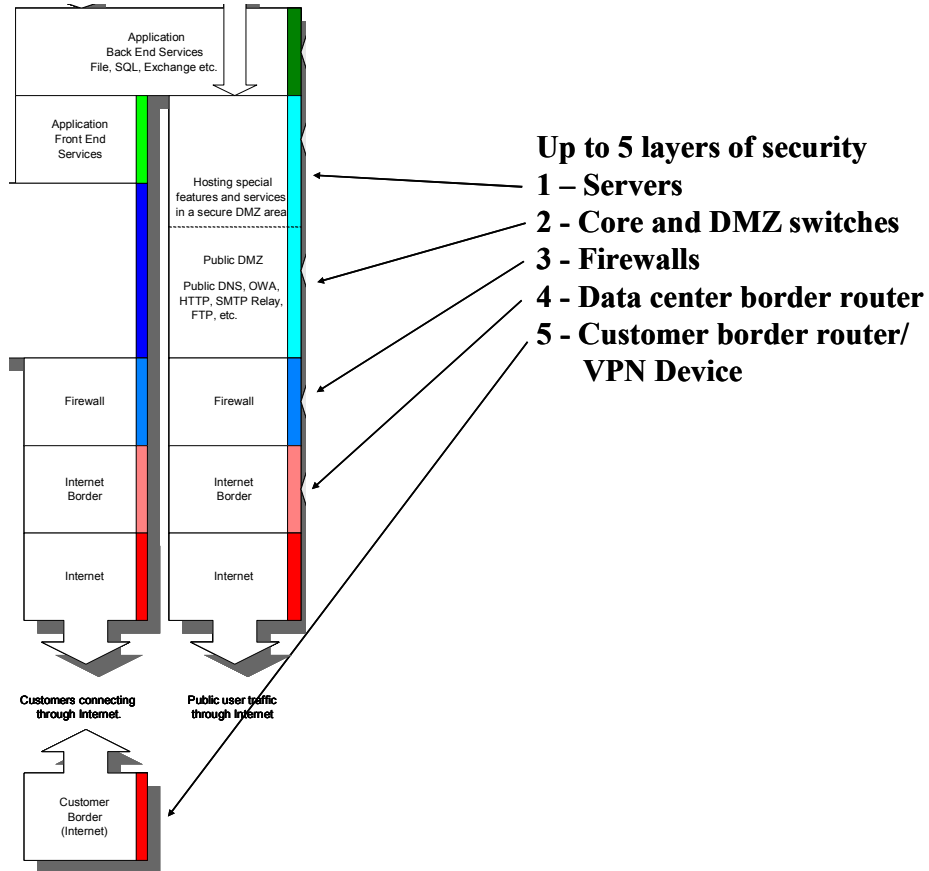
Recognizing the scope and depth of security issues that a technology business faces today, we are teaming with other organizations to keep abreast of the latest security issues, tools, tactics, ideas and laws. This includes InfraGuard, formed by the United States of America's Federal Bureau of Investigation (FBI) and the National Infrastructure Protection Center (NIPC). InfraGuard is a cooperative group with membership from business, academia, state and local law enforcement agencies and other entities. InfraGuard is dedicated to sharing the knowledge and experience of this broad base of membership, with the objective of increasing the security of the nation's critical infrastructures. Additionally, our security professionals enjoy membership in a variety of professional organizations such as the High Technology Crime Investigation Association and the Information System Security Association.

7 Technical Security Measures

This section describes the technical security measures that have been put in place to fulfill the Security policies and processes derived from ISO-17799 as our security standard. Technical security measures fall into three primary categories:

- Network Security
- Host & Application Security
- Subscriber Access Security

The security measures supported within each of these three categories combine to create a multi-layered approach to technical security as shown in the diagram below.



Each of these categories is described in the sections below.

7.1 Network Security

Security is a major consideration for the hosted Exchange network environment. Sensitive information such as e-mail and scheduling are stored on the ASP's servers and thus become targets for malicious attacks mounted over the unfortunately handy communications paths of the Internet.

Securing sensitive information in this environment requires that data is sent securely over the Internet from the client to the hosted Exchange environment and vice versa. In addition, the hosted Exchange environment itself, which stores the sensitive information, must be secured from attacks from the Internet.

7.1.1 Message Encryption

There are two ways that information sent on the Internet is secured in the hosted Exchange environment. For Web-based OWA e-mail, Secure Sockets Layer (SSL) encryption is used. At the beginning of each session, the browser on the client negotiates a secure tunnel with the OWA server ensuring that all data sent between the client and the OWA server is encrypted. For MAPI-based e-mail using a full Outlook client, RC4 encryption is used.

The Outlook client has a built-in encryption mechanism that encrypts the MAPI data portion of the packet sent on the Internet. By encrypting only the MAPI data portion of the packet, the sensitive data being sent is encrypted, while the protocol portion of the packet remains in clear text. This allows the packets to be inspected by the ISA Server Exchange RPC application filter upon entering the hosted Exchange environment.

7.1.2 Perimeter Security

Perimeter security measures protect the data center network infrastructure from unauthorized access from the public internet or other private network connection. Firewalls, Proxy Servers, Virtual LANs, and Network Address Translation features all provide key capabilities with regard to the enforcement of perimeter security, and are described in more detail below.

7.1.2.1 Firewalls

Data center production networks are protected by Cisco PIX firewalls. A firewall is a mechanism for controlling the flow of data between two parts of a network that are at different levels of trust. The Cisco PIX firewalls inspect traffic between our front-end and back-end networks.

7.1.2.2 Proxy Servers

The reference architecture uses perimeter security to secure the hosted Exchange environment from the Internet. ISA Server provides proxy-based perimeter security. ISA Server, being able to inspect packets up to Layer 7, provides robust security, dropping any unwanted packets and preventing them from entering the hosted Exchange environment. Hosted Exchange Customers using MAPI are protected with the Microsoft ISA Server product which provides MAPI port filtering producing a High Availability and Highly Secure service offering.

7.1.2.3 Virtual LANs

Extensive IP subnets/VLANs with designated roles are used for enhanced security of the network. The role of a specific subnet will dictate which ports and protocols are allowed to traverse that subnet. Those ports and protocols that are not required within a subnet are specifically prevented from traversing the subnet. For example, DNS and SMTP provider resources are reachable at an IP traffic layer only by devices that have an explicit and specific need to contact those resources. SQL Cluster and Exchange Cluster Back Ends are treated similarly, as are terminal servers and Exchange Front End servers. Virtual Private Networks, frame relay and dedicated lines are used where appropriate to security network connections. For users of Outlook Web Access, connections are protected by 128 bit SSL.

7.1.2.4 Network Address Translation (NAT)

Network Address Translation allows a single device, such as a router, to act as an agent between the Internet (or "public network") and a local (or "private") network. This means that only a single, unique IP address is required to represent an entire group of computers. This also provides an addition level of security by shielding the IP addresses of devices on the internal network. If hackers don't know the internal IP address of a server, then it's harder to attack it.

Traditional firewalls can act as a boundary for IP addresses, using Network Address Translation (NAT), preventing DoS by limiting traffic using specific TCP ports, limiting traffic coming from specific network addresses, or even scanning traffic for viruses or undesirable applications. However, traditional firewalls do not scale well for today's extremely high-traffic Web environments.

Our network architecture leverages hardware load balancing switching, which provide the following additional security capabilities, including Network Address Translation.

- Denial of service (DoS) attack prevention
- Traffic filtering (by IP address, TCP port, Host Tag, complete URL, or file type)
- Network Address Translation (NAT)

7.1.3 Denial of Service (DoS) Attacks

The challenge for successful public Web sites is to encourage access to the site, while eliminating undesirable or malicious traffic, and providing the necessary levels of sufficient security without creating constraining site limitations in performance or scalability.

Disruption of service caused by denial-of-service (DoS) attacks is the "kiss of death" for Web-driven enterprises such as portals and e-commerce sites. The 1999 Computer Crime and Security Survey found that system penetration by outsiders increased for the third year in a row, with 30 percent of respondents reporting intrusions. Those reporting their Internet connection as a frequent point of attack rose for the third straight year, from 37 percent of respondents in 1996 to 57 percent in 1999.

Preventing DoS attacks is critical for most Web sites. These attacks are specifically designed to bring down a Web site using methods that appear to be normal network traffic—until it is too late. Web-site administrators have used packet filtering in their IP routers to provide basic access control, but often this slows router performance to an unacceptable point and fails to eliminate many common types of DoS attacks.

Today's load balancing switches provide comprehensive front and back-end system security capabilities designed to provide the right level of security without sacrificing scalability or performance. Load balancing switches are designed from the ground up to provide comprehensive solutions for all aspects of security without compromising performance or scalability. They combine the inherent intelligence to eliminate sophisticated DoS attacks with the flexibility to configure custom security policies, ensuring the constant availability of the site for real customers and legitimate users.

7.1.4 Spam Prevention

7.1.4.1 Outgoing

We exercise every commercially reasonable effort to prevent user spamming from the email system, including but not limited to, limiting the number of addresses in the address fields (To: cc: bcc), limiting the number of users in a single group in the address group, blocking a particular end user's email account at the request of the customer, and providing customer with an online administrative tool that shall enable editing, modifying and deleting specific end user accounts at its discretion. We also reserve the right to block specified accounts that we feel are violating our spam policies.

7.2 Host & Application Security

7.2.1 Server Security

Servers are hardened by an internally developed automated methodology. Only those operating system services that are specifically required on a server are allowed to run. Every user-accessible component, including terminal servers, web servers, file servers, or any other Microsoft OS-based computer placed in the production environment, has each and every file permission set explicitly with a focus on maximizing availability and minimizing exploitability. The hardening method includes the rigorous application of NTFS permissions as well as local security policy options, domain security policy options, and individual group security policy options. This stringent analysis and evaluation of all Windows 2000 security policy options, numbering in the thousands, insures that hosted companies are protected not only from their own malicious internal users, but from each other as well.

7.2.2 Malicious Software Security

Precautions are required to prevent and detect the introduction of malicious software. Software and information processing facilities are vulnerable to the introduction of malicious software, such as computer viruses, network worms, Trojan horses and logic bombs.

Data Centers are protected by Trend Micro's "ScanMail" and "Virus Wall" products, which detect and remove inbound and outbound viruses in real time. Email attachments are scanned prior to a user having the opportunity to access them. Uncleanable viruses are quarantined. Engineers receive timely

notification of emergent events (for instance, an unusually large number of viruses are received during a short period of time). Antivirus software is automatically updated hourly or more frequently when warranted. Engineers confirm the successful automatic application of new virus signature files.

In addition to the anti-virus protection described about, the following controls have been implemented to protect against other types of malicious software and prevent their introduction into the production service delivery environment.

- A formal policy requiring compliance with software licenses and prohibiting the use of unauthorized software is enforced
- A formal policy requiring compliance with software licenses and prohibiting the use of unauthorized software is enforced
- A formal policy to protect against risks associated with obtaining files and software either from or via external networks, or on any other medium, defines what protective measures should be taken
- Regular reviews of the software and data content of systems supporting critical business processes are conducted. The presence of any unapproved files or unauthorized amendments are formally investigated
- Files on electronic media of uncertain or unauthorized origin, or files received over untrusted networks, are checked for viruses before use

7.2.3 Multi-Tenancy

Securing a multi-tenant environment that provides messaging services to multiple customers on a single shared infrastructure is a critical service delivery requirement. The primary technical mechanism for securing each customer so that no customer can see any information belonging to another customer is through Directory Security. Directory security allows us to secure a customer's Organizational Unit (OU) in a way that allows the administrators and users for that customer to see all objects within the OU, but not be able to see objects outside of their OU.

This directory security is different from file-level security. Directory security restricts what a set of users can see and list in the directory, whereas file-level security blocks them from accessing certain information. If you secure your directory correctly, one customer cannot view or list the information of another customer. For example, you can restrict Address Book lookups to a specific organizational unit and, therefore, to a specific hosted customer. Using directory security, you can delegate security for each customer, or organizational unit, separately.

Directory security also restricts what a user can see in the directory. Because a shared-directory model is structured so that users in all hosted companies reside in the same instance of Active Directory, it is important to set up a directory structure that grants the appropriate access permissions to each group of users. If you set up security correctly, users can see only information regarding their own customer.

The following diagram illustrates how this works.

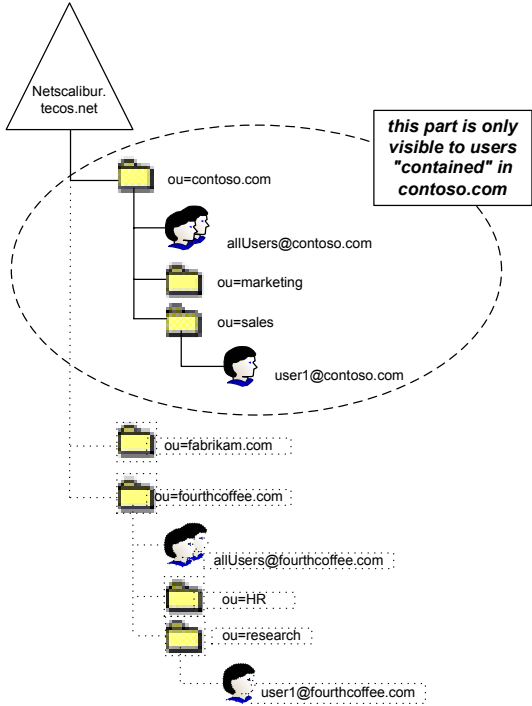


Figure 1 - Active Directory Partitioning through OU Permissions

Active Directory uses the following mechanisms to determine the extent to which users can access network resources:

- **Access control lists (ACLs)** — a list of permissions that control which users can view and access objects (OUs, the domain root, user objects, and so on) in Active Directory.
- **Access control entries (ACEs)** — the individual permissions that make up the ACL and contain permission entries such as Read, Write, Execute, List Content, and so on. You can use ACEs on both the directory and Exchange 2000 configuration objects to restrict or allow access to services such as address books and viewing membership.
- **Security policies** — policies that define the security functionality of the system. By using Group Policy objects in Active Directory, administrators can centrally apply explicit security profiles to OUs within the directory.

Directory security also applies to the permissions we give to our customer administrators. These administrators can only be able to administer their company’s portion of Active Directory, and not the entire directory. TECOS™ AdminCenter provides this capability through a web-based user interface.

7.3 Secure Access Capabilities

Another important aspect of our security program is the ability to securely access the service over the public Internet. A variety of different secure access methods are provided that allow secure, encrypted access to the hosted messaging environment. These methods include the following:

- MAPI Connectivity using a Virtual Private Network (VPN)
- “Published” MAPI
- Outlook Web Access
- AdminCenter & UserCenter

Each of these secure access methods is described below.

7.3.1 MAPI Connectivity

The Messaging Application Programming Interface (MAPI) protocol provides a feature-rich set of functionality for accessing Exchange. MAPI is a de facto Microsoft system standard for messaging and workflow applications. In addition to being able to access all of the mailbox’s folders as well as public folders, MAPI clients can access electronic forms, the Calendar, Journal, Contacts, Task List, and Notes components. In short, MAPI provides a far richer interface to the Exchange server than HTTP, POP3, or IMAP4.

The two methods of secure MAPI access – VPN and Published MAPI – are described in the sub-sections below.

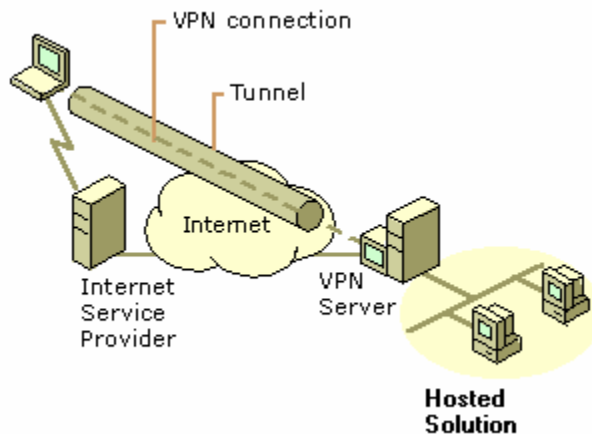
7.3.1.1 Virtual Private Network (VPN) Access

Virtual Private Networks (VPNs) provide secure network services over a public network, like a private network does, but at a reduced cost. VPNs allow company staff and other authorized users to connect to the hosted solution from remote locations as securely as they can from a company site. Therefore, all hosted services can be securely offered over VPNs. VPNs require more effort than non-secured public connections to understand, set up, and support, but they provide fully secure connections using low-cost Internet or similar connections.

7.3.1.1.1 Remote Client Option

Virtual private networks typically work as follows:

- The user connects to any Internet service provider (ISP).
- The VPN client software contacts a designated VPN server owned by your company through the Internet and initiates authentication.
- The user is authenticated and security details are provided.
- The VPN server provides a new Transmission Control Protocol/Internet Protocol (TCP/IP) address to the client computer and the client computer is directed to send all further network traffic with that address through the VPN server.
- All network packets are then fully encrypted as they are exchanged in a manner that only the VPN client and VPN server can decrypt.



7.3.1.1.2 Persistent Connection Router-to-Router VPN

Persistent Connection Router-to-Router VPN A router-to-router VPN is typically used to connect remote offices when both routers are connected to the Internet through permanent high speed WAN links. In this type of configuration, you only need to configure a single interface on the customer router and the hosting provider’s router. Permanent connections can be initiated and left in a connected state 24 hours a day and provide the same level of encrypting over the public internet as the client side VPN

option. This option is best suited for small to medium size customers, the do not want to incur the expense of a dedicated connection to the service provider.

7.3.1.2 “Published” MAPI

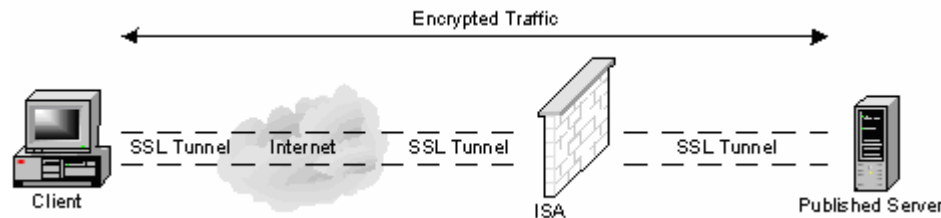
One of the greatest features of ISA Server is its ability to publish Exchange Servers, allowing access over Remote Procedure Calls (RPC). ISA Server is currently the only firewall on the market that has a specific Exchange RPC application filter capable of securely publishing Exchange services. Using this capability, MAPI/RPC data is exchanged from a full MAPI/Outlook client on the Internet to a published Exchange Server shielded behind ISA. By combining this functionality with the ability of Outlook to encrypt RPC data, your hosted users no longer need to VPN into the hosted network, but can access their e-mail via Outlook directly from the Internet.

SSL encryption is widely used on the Internet to encrypt data flowing between a client and a server or a server and another server on the Internet. Because the Internet is inherently insecure, it is important to encrypt any type of personal, sensitive, or proprietary information that is transmitted.

By using certificates, SSL also ensures identity. Certificates are issued by trusted certificate authorities that guarantee the true identity of a certificate bearer. Web sites that allow SSL encryption typically obtain a certificate from a trusted Certification Authority (CA) service such as VeriSign, Entrust, or Thawte. By connecting to these Web sites via SSL, the third-party CA vouches that the Web site you are connecting to is the intended Web site and not a hijacked site.

ISA server uses SSL is to create a protocol definition for Inbound SSL (Port 443) then create a new server publishing rule that uses the “Inbound SSL” protocol definition. This type of implementation passes through an SSL connection from a client on the Internet to a destination server. Clients still connect only to ISA Server. ISA Server then connects to the destination server and forwards the encrypted packets to the destination server. ISA Server does not inspect the contents of the packet because it is encrypted using a Public Key Infrastructure (PKI) encryption that is decrypted only at the client and destination server.

The diagram below shows how an Outlook 2002 client connects to the hosted messaging service using “Published” MAPI.



7.3.2 Outlook Web Access (OWA)

OWA front-end servers are by definition a layer of security in the Application Service Provider (ASP) design. By proxying HTTP requests, the servers accept connections from the client and proxy the requests to a back-end Exchange Server computer. In this way, the OWA client never directly connects to the back-end computer running Exchange Server.

In addition, OWA front-end servers allow access only through Secure Sockets Layer (SSL) encryption.

7.3.3 AdminCenter & UserCenter

TECOS™ AdminCenter and UserCenter provide the ability for customers and end-users to self-administer the Hosted Messaging and Collaboration services, including password resets, and other service administration actions. Secure access to this site is critical to the overall security of the services and delivery platform.

Access to the AdminCenter and UserCenter web-based user interfaces is only permitted through Secure Sockets Layer (SSL) encryption.