Global Information Assurance Certification Paper

GCFW Certification

Mark Rubino

GCFW Version 4.1
Assignments

Date: Mar. 24, 05

Securing Voice over IP (VoIP)

Written by: Mark Rubino

March 18, 2005

Voice over IP (VoIP) is quickly growing in deployments across both the commercial and residential markets. The promise of this converged communications, the delivery of voice on the data network, includes cost savings, flexibility and improved communications. In the past with many technologies the rush to deployment at times left security as a secondary concern – until the first incident. VoIP security must be introduced from the beginning stages of design, followed through deployment and finalized with validation testing and a maintenance policy. Failing to do so could leave service affecting vulnerabilities not only for the VoIP network but open the data network to exploitation as well. This paper will discuss VoIP security concerns and recommendations to correct or minimize vulnerabilities during typical deployments.

H.323 Background and Definitions

Today users have a choice between equipment and protocols for their VoIP deployment, the International Telecommunications Union (www.itu.org) H.323 and a promising newcomer the Internet Engineering Task Force (www.ietf.org) Session Initiation Protocol (SIP). The majority of existing VoIP equipment and deployments today utilize H.323 and this will be the focus of the paper.

The ITU released H.323 version 1 in 1996 (at version 5 in 2003). The recommendation is actually composed of several elements and protocols designed for multimedia communications over packet networks. Proposed for multimedia, the typical deployment today focuses mainly on the delivery of voice. Vendors are free to implement in hardware or software. Only the components and protocols discussed within the paper are referenced below. The following descriptions were referenced from http://www.dialupaudio.com/h323primer.html .

Gatekeeper - provides network services, admission control and authentication of H.323 devices into their network. Controls the administration and configuration of ip attached Terminals. Gatekeepers are considered optional equipment.

Gateway - provides the conversion between H.323 devices and non-H.323 devices (ip phone to PSTN network or digital and analog phones attached to the system). Call signaling (and other non-media related tasks) and interface to other H.323 networks.

Terminals - are the IP hardphones (telephones), IP softphones (a PC based phone application) Voicemail systems and call center systems.

H.225 - provides two functions – with the Gatekeeper it defines the Terminal registration (RAS) and is used for call setup and teardown with Q.931, H225 providing additional information within Q.931. Call setup can be between Terminals and Gateways or directly between Terminals (IP enabled). H.225.0 RAS messages are defined using the ASN.1 notation (X.680).

H.245 - utilized to coordinate and negotiate the direct media path setup (the RTP VoIP channels) between Terminals after call setup via H.225 and Q.931.

Q.931- used for call signaling (setup and teardown) in ISDN networks. It is used to setup and teardown H.323 calls as well. During call setup imbedded in the Q.931 messages are H.225 messages providing additional information necessary.

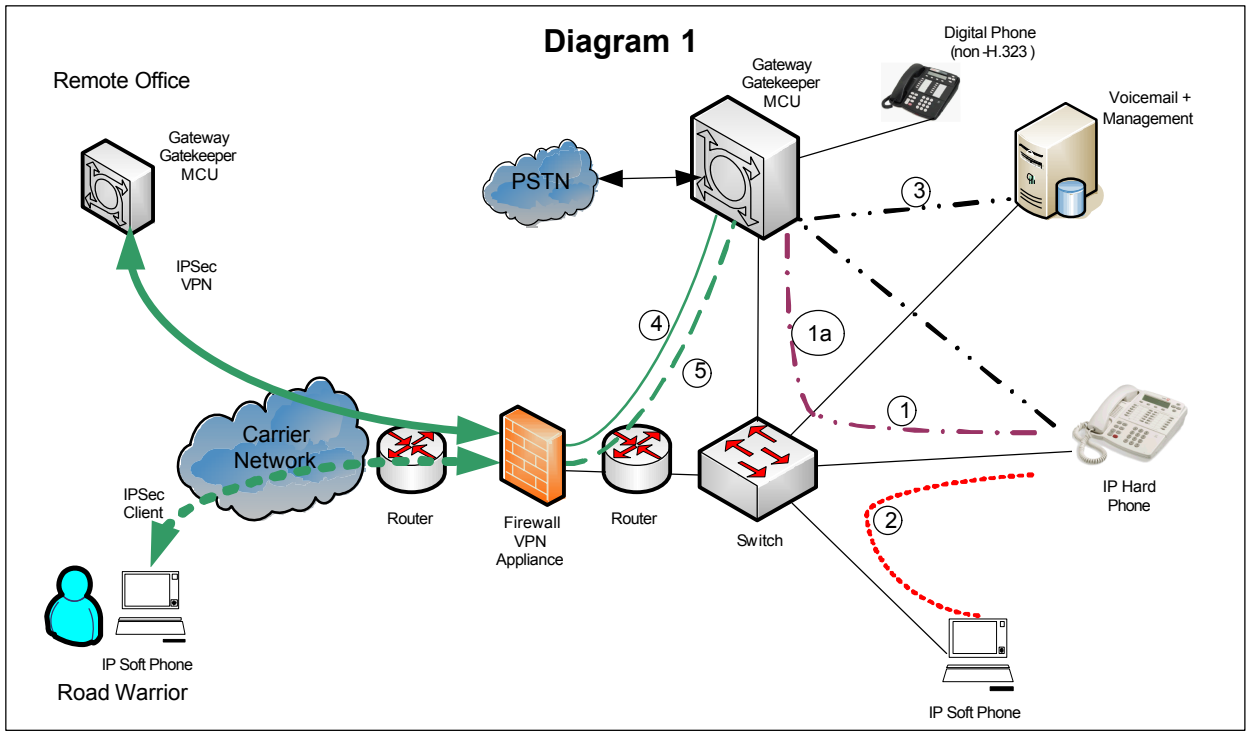
RTP - the workhorse protocol from the IETF used to pass the digitized media information between Terminals (the conversation data). Due to their strict delivery requirements vendors mark RTP packets with an IP DSCP (IETF rfc2474, rfc2475) for prioritized delivery through the network.

Auxiliary Equipment
No telephony system deployed in business today would be complete without at least a voicemail and a management system. Additions to this may include an auto-attendant (thank you for calling ABC industries, press 1 for sales...) and call center applications (for collecting Gateway statistics and providing reports on call use for trend analysis). Many vendors also offer advanced Computer Telephony Applications (CTI) and Integrated Messaging Systems (IMS). CTI can provide PC based interfaces for controlling the physical phone as well as status and monitoring of a group of telephones. IMS can provide features such as voicemail to email notification, retrieval and playback. It's important to remember vendors are free to implement and inter-connect these systems to the main H.323 system (Gateway and Gatekeeper) via any method of their choosing using H.323 or other TCP/IP mechanisms.

H.323 Typical Deployment and Operation - Diagram 1
This section will provide an overview of H.323 interconnectivity found in a typical network. It is important to understand the network deployment, H.323 flows and device interactions. Only with this understanding can vulnerabilities be identified and methods to minimize or prevent them formulated. The following is representative of the majority of vendors' equipment operation.
NOTE - Vendors can vary in protocols and connection methods for functions outside the H.323 standard. They may use H.323 or follow methods other than our example.

DHCP
Most venders support DHCP on their H.323 terminals (IP telephones) for ease of IP address assignment, configuration and deployment. DHCP may be provided by the vendors H.323 equipment / application, such as the Gatekeeper/Gateway, or by another DHCP server on the network.

TFTP
Vendors use TFTP throughout their equipment for configuration updates and changes (online and offline) as well as code updates to equipment when necessary. The TFTP server can be a part of the vendors H.323 equipment / application or another server on the network.



IP Terminal to Gatekeeper (RAS) ① (UDP1719, TCP1720, H.225, Q.931)
When power is applied an H.323 terminal (IP Phone) depending on its programming may initiate DHCP and then TFTP – first obtaining an IP address and then checking for possible code updates or configuration data. Next is registration to the Gatekeeper via a UDP port 1719 connection to pass H.225 RAS messages. Once registered the IP phone initiates a connection with TCP port 1720 for exchanging H.225 and Q.931 messages with the Gateway to set parameters such as set type, country code, extension number, etc. With registration complete the IP phone can now make calls.

IP Terminal Calling (non-H.323 phones or PSTN) 1a (TCP1720, H.225, Q.931, RTP)
Going off-hook the IP phone initiates a TCP port 1720 connection to the Gateway. This passes H.225 and Q.931 call setup data. Gateway programming determines the call is for a non-H.323 phone or PSTN line call. Also started and established are RTP connections for communicating the voice data between the Gateway and IP phone. The RTP connection is negotiated using any UDP port above 1024 - the starting port or port range used is vendor specific. Once the call is connected the Gateway is used to convert the analog voice via a codec to the RTP connection between itself and the IP phone. The IP phone has a built-in codec for the packet to analog voice conversion at its end.

IP Terminal Calling (RTP direct media path) ② (TCP1720, H.225, Q.931, H.245, RTP)
The initial call setup proceeds as described in the section above to non-H.323 phones. System programming and information elements passed during RAS and call setup

may allow for direct RTP connection between IP terminals. If allowed the IP phones are passed info via H.254 from the Gateway to negotiate and establish direct RTP data streams between each other without using the Gateway.

Voicemail (internal) ③ (TCP1720, H.225, Q.931, UDP)
Before leaving a voicemail message the IP phone follows call setup as described in 1a to the Gateway. This is logical as the IP phone is trying to establish a call. After a system or user defined time limit the Gateway will 'timeout' the call to the phone and redirect it to the Voicemail system. The Gateway now sets up a UDP connection to the Voicemail server, specifying which 'mailbox' to place the recording in (the UDP port used is vendor specific). The Gateway provides the conversion from the phone RTP stream to the vendor message record protocol. When retrieving a voicemail message the phone begins with call setup (1a) and passes a code specifying 'connect to Voicemail', directing the Gateway to set up the UDP connection to the Voicemail system for recording (voicemail) retrieval. Note that when either a non-H.323 terminal attached to the Gateway or an inbound call from the PSTN requires a call be directed to voicemail, the Gateway will use the UDP connection between it and the Voicemail described above.

Gateway to Gateway Calling ④ (TCP1720, H.225, Q.931, RTP)
Gateways can be connected via several methods; dedicated line, Frame Relay and even Internet accessible DSL (though there may be VoIP quality issues). Each Gateway is programmed for connectivity to the other Gateways; IP addresses, routes, calling plan, etc. (this is vendor specific). Gateway's establish call setup to each other via the same H.323 flows as described between Gateways and IP phones - TCP port 1720 (H.225 and Q.931) and RTP. The local gateway is responsible for connectivity (and VoIP conversion if necessary) to its directly attached phones or PSTN circuits.

Remote IP Phone ⑤ (UDP1719, TCP1720, H.225, Q.931, RTP)
H.323 Terminals can be remotely located from their Gateways via the same methods used for remote Gateways. Remote terminals can be IP Hardphone or Softphone. Whether IP Hard or Softphone they will follow the H.323 procedures and protocols described earlier in our examples (1, 1a, 2 and 3).

Management (TCP, UDP, HTTP)
All vendors will provide an interface to their equipment for configuration and troubleshooting. They use existing TCP, UDP or HTTP LAN connection methods from the management platform or in rare instances DTE terminal communications.

H.323 Vulnerabilities
Like any communications technology H.323 has vulnerabilities – in the protocol itself, in vendor software / operating systems and in methods and devices used in an auxiliary role. H.323 vulnerabilities can be classified into two main categories: Denial of Service (DoS) which includes distributed denial of service (DDoS) and Arbitrary Code

execution on an operating system (OS).

VoIP DoS can be separated into two distinct types – unintentional and intentional. Unintentional DoS could result from simple misconfiguration of a VoIP terminal or other network device, preventing registration, communication and callsetup to the Gatekeeper/Gateway. Another example would be a user opening an infected email attachment. As the virus attempts to propagate through the network to infect other's the increase in traffic can interfere with VoIP network operation. The increased traffic can prevent RAS registration, RAS keepalive, call setup could be delayed, and conversations could suffer missed words from dropped or corrupted RTP packets.

Intentional DoS is just that, a deliberate attempt to send information to a system or endpoint in the VoIP network to prevent or hamper normal operation. These can range from well know attacks such as a high rate of ICMP traffic or specially crafted packets exploiting known H.323 issues. The University of Oulu in Finland has tested several vendor offerings of with a unique testing process called PROTOS. The report provides one of the most comprehensive listings of H.323 vulnerabilities and is recommended for those developing code or deploying H.323 services. The complete report is available for viewing at http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/h2250v4/index.html

One example listed in the report would be an H.323 packet crafted with a "Q.931-calling-number-digits-overflow". Some vendors upon receiving this packet will reboot.

The report provides insight into the complexity of an H.323 packet and the various elements that could be vulnerable. Although done some time ago there is always the possibility that many vendors have not corrected for all the vulnerabilities listed. In addition new as yet unknown vulnerabilities can be introduced with each new release of H.323 code.

DoS – unintentional or intentional - at any level of occurrence could quickly render the VoIP network unusable and its impact can not be understated. DoS at levels considered a nuisance in data networks can have severe impact on VoIP due to the time sensitive packet delivery of the RTP stream.

Arbitrary code execution is more likely to impact vendors with code/software based Gateways and Gatekeepers. The vulnerabilities extend to the hardware and underlying operating system the software runs on. Hardware based H.323 components may be vulnerable to some extent depending on the underlying OS used by the vendor. Recently in the press we see increased concern regarding IP Softphones and possible compromise, infection and access to the root operating system (http://www.computerworld.com/securitytopics/security/story/0,10801,99258,00.html).

As yet there hasn't been comprehensive testing of IP Softphone vulnerabilities as done with PROTOS and H.323 but as seen before with client applications the possibility of 'buffer overflows' and other similar exploits can exist.

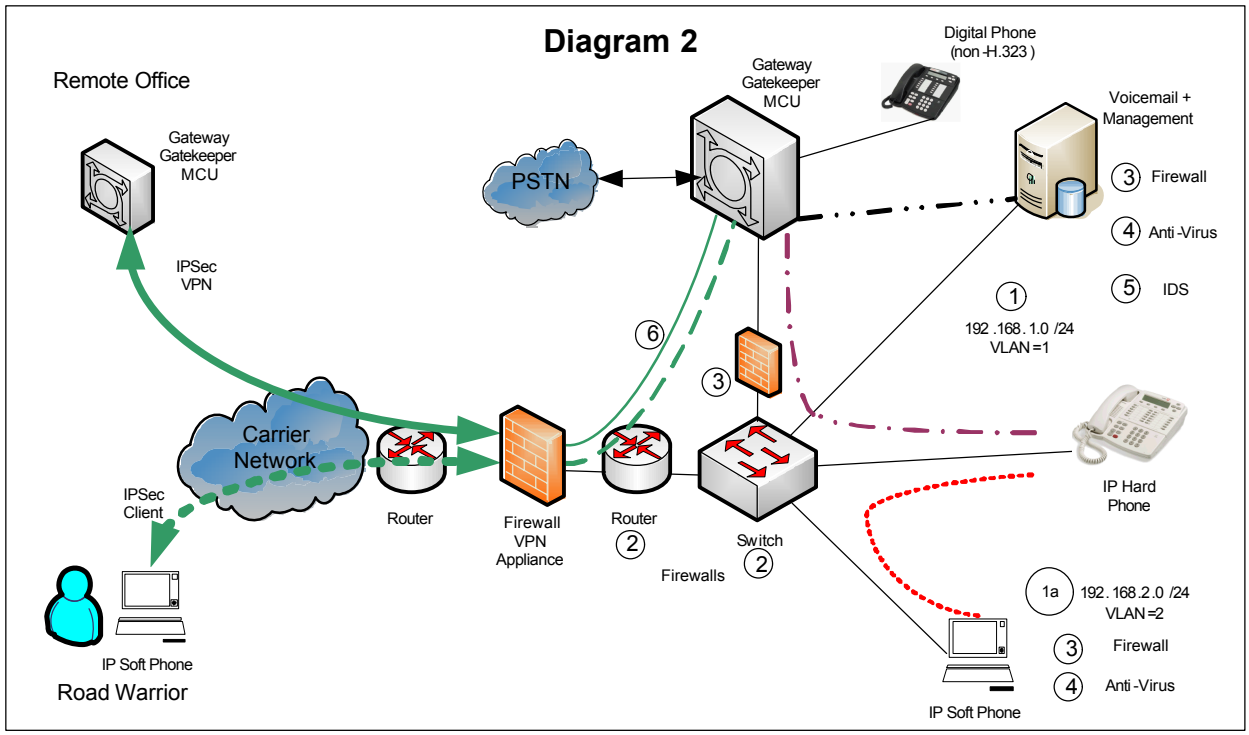
Vulnerability due diligence must be extended to the supporting protocols mentioned in the 'typical deployment and operation' section and any other protocols used by your specific vendor. These protocols contain their own vulnerabilities and exploits, the reason for their inclusion in the earlier section. Issues with the protocols deployed in support of H.323 networks (DHCP, TFTP) have been noted and discussed in our industry before and will not be belabored here.

A vulnerability often seen in the field but overlooked by many is the traditional

separation between the voice and data engineering organizations. In large companies voice and data are separated into two organizations each with distinct responsibilities and expertise. VoIP may at times be thought as by data engineers as 'simply voice' and voice engineers may not be familiar with the security concerns of IP networking. In large firms the data security personnel should be notified of new equipment and server installations and have in place existing policies to apply to the deployment. This vulnerability is most prevalent in small to medium businesses using outside consultants, one for data networking and one for traditional voice networking. In this scenario it's highly likely for a breakdown in communications. Who owns the responsibility of the overall security integration? Continued education and training across these traditional engineering domains is necessary.
It's possible to fill the remainder of the paper discussing details of H.323 exploits and vulnerabilities but that is not the goal. The 'References' section provides websites as a starting point for review regarding known H.323 exploits and vulnerabilities. Be sure to include your vendor's website for the latest vendor specific alerts and an Internet search of "voip vulnerabilities" will produce interesting results as well.

Securing Voice over IP

We have reviewed H.323's protocols, operation and provided examples and references regarding exploits and vulnerabilities. It's time to recommend multi-level processes and procedures which will provide a defense-in-depth for an H.323 network. What do we need to secure against? Start with protection from the list of H.323 vulnerabilities; unintentional-intentional DoS and Arbitrary code execution. In addition control anything and everything not associated with the normal operation of the VoIP network because you never know where the next vulnerability or exploit will come from. Refer to Diagram 2 as you review the recommendations.



IP Subnetting or VLAN's (1) (1a)

Separation and isolation of the H.323 and data network is a must to be included in your deployment planning. This is an essential first step defensive measure for any H.323 network. Probability states a virus attack is most likely initiated, intentional or not, from the data network, the benefits of separating the data and VoIP networks is clear. This can be accomplished via IP subnetting or if your network equipment vendor supports them - VLAN's. A word of caution if you are contemplating VLAN's, ensure your vendor can provide advanced functionality that can limit and control connectivity between VLAN's. Isolating the VoIP network will provide two benefits; isolation from extraneous data traffic for better VoIP quality and hinder or prevent virus impact (DoS) and spread to the VoIP equipment (though this is not a guarantee, depending on the virus propagation method). Subnetting and VLAN's also can provide operational and administration separation of H.323 network specific supporting infrastructure such as DHCP, TFTP and any auxiliary applications and servers. Subnetting or VLAN's allows us to put in place the next level of defensive measures.

Firewalls (2) (3)

Include plans for deploying firewalls in your H.323 network to limit traffic and packet flows between the VoIP and data networks. Depending on the H.323 equipment deployed these may need to be a combination of network and/or host, hardware and/or software based. All firewalls directly related to the H.323 flows (RAS, Callsetup, etc) should be stateful firewalls. Packet filters with "ip>any>any" rules will not do. Referring to the "Typical Deployment and Operation" section, H.323 RAS and Callsetup destination ports are well known but not the initiator or return ports. The RTP streams

are in no way referenced by the H.323 TCP1720 connection. An H.323 aware stateful firewall is a must. In Diagram 2 a host based firewall is needed on the Voicemail/Management (software based) server. The Gateway/Gatekeeper (hardware based) will need a hardware based network firewall installed③. Depending on the vendor's switch and router this may be a module or software available for installation within the network devices②. This is needed due to the deployment of IP Softphones on the data network PC's and remote Gateways. All firewalls rules should be 'fine tuned' to allow connectivity only between the IP addresses and ports involved in H.323 network operation. This will minimize intentional (specially crafted H.323) exploit packets from other sources, providing a defense against this type of DoS attacks. Some firewall vendors H.323 support does allow for dynamically opening ports and connections for the RTP streams. If not an RTP packet stream a rule can be defined to allow the IP address, expected vendor's UDP port range as well as matching the specific DSCP marking in use. The Voicemail and Management server could possibly use a packet filter firewall, its only communications being to / from the local Gateway. Its rule set allowing only the Gateway IP address and vendor TCP/UDP port range. Continue to build firewall rules to include any vendor specific interconnectivity between the Gateways and Auxiliary servers and the broader network management systems. This is where knowledge of your vendor equipment and operation becomes important.
Network firewalls may not be necessary. In the example network there are remote Gateways and IP Softphones but in some deployments there may not, negating the need for any access from outside the stand alone H.323 subnet. In these cases security may be provided by simple vendor available programming rules preventing any ip connectivity between the VoIP and data subnets except for management.

Host based Anti-Virus Software ④

Any vendor software based H.323 element or supporting application deployed on a PC, workstation or server should include a host-based anti-virus package. Vendors recommend or require that the application and system be dedicated and security practices dictate that only the administrator have access to this system – never the less it is not impossible that the system could be the target of a virus. The example network includes a host based anti-virus package on the Voicemail server. The anti-virus software should be programmed to run checks on a daily basis at a time that would least interfere with the Voicemails normal operation. In addition you should consider disabling the "on access scan" feature of the anti-virus for the voicemail directories. Failure to properly configure the anti-virus risks creating a "voicemail DoS" of your own making through high CPU utilization.

Host based in IDS ⑤

Any vendor software based H.323 element or application deployed on a PC, workstation or server should include a host-based Intrusion Detection System (IDS). As stated in the anti-virus recommendation this should be dedicated and a limited access system but needs to be monitored against intrusions. In certain aspects this system could be a prime target for intrusion due to its generally un-monitored operation. The example network deploys a host based IDS on the Voicemail/Management server.

Ensure the IDS selected monitors and alerts to the OS specifics of your deployment. The IDS should alert the administrator to changing registry entries (Windows based), users (or root privileges) and new applications and files. In our example Voicemail system, we expect communications only from the local Gateway and changes to voicemail message files (in the Voicemail application directory) as messages are left and deleted. Knowledge of your vendor specifics will allow for fine tuning the IDS and a quick review of the reports.
*note – A network based Intrusion Detection System should be installed. Since this is not H.323 network specific it is not covered in this document.

IPSec Tunnels ⑥
The network includes remote sites each with a Gateway to allow inter-office calling and a number of remote users with IP Softphones – telecommuters and a sales force. Assume our Carrier Network is providing a virtual LAN offering with the network providing interconnectivity for all sites VoIP, data and internet access. Regardless of the Carrier's claims of separation and isolation of their offering the Gateway sites and remote users should be connected via IPSec tunnels, especially for the Internet connected IP Softphones. Addition of a Firewall/VPN or separate VPN appliance should be deployed in the network to support this. IPSec tunnels will provide the conversations with security from eavesdropping (with or without H.235v3) and improved isolation from attack and penetration. Internet access allows remote users a secure connection (via an IPSec client) to their corporate Gateway to make and receive calls as if they were on their office phone. In addition the IPSec tunnel (operating in tunnel not transport mode) allows the use of non-routable IP addresses (IETF rfc1918) in the internal VoIP network with no NAT (Network Address Translation – IETF rfc3022) issues. H.323 does not NAT well, the H.323 devices IP addresses are embedded in the H.225 messages, unless the vendor offers special code to circumvent this. There are VPN, Firewall and Application Layer Gateways available today that can NAT H.323. Some work with specific H.323 vendor's while others claim operation with any H.323 equipment. In some cases NAT is accomplished by programming and terminating the Gateway's VoIP trunk to the local NAT appliance instead of the normal configuration of directly connecting to the remote Gateway (Gateway > local appliance >< remote appliance > remote Gateway). The NAT function is accomplished between the appliances. This adds an additional 'hop' between the Gateways. Check with both vendors (VoIP and Appliance) to thoroughly understand and test this functionality with your equipment before deployment. The overall WAN design and technology used for interconnectivity between remote Gateways and elements will decide on the validity and placement of IPSec tunnels in your VoIP network.

Security Architecture – Testing, Integration and Maintenance
After all components are installed and operating the security of the VoIP network should be validated with a network security assessment. Ensure all components function as designed and configured, providing the security expected while not inhibiting the operation of the VoIP equipment. Establish procedures and policies for the VoIP security components. All components must have security reviewed on a scheduled basis - logs checked, passwords changed, code and security updates

completed regularly. Establish and exercise system backup and recovery procedures for the VoIP equipment in the event of a "zero day" exploit. Going several hours without email can be a nuisance, going several hours without the ability to make or receive calls can be catastrophic. While the recommendations focus on H.323, all generally accepted data security practices must apply. The VoIP network should be integrated into the overall network security architecture and procedures already in place. VoIP inclusion into established security procedures will ensure proper operation between VoIP and data network security equipment. Integration can also provide additional layers of defense for the VoIP network such as already deployed network based IDS, Firewalls, secure log servers etc.

VoIP Security

VoIP security is definitely coming to the forefront of the industry. A number of vendors have recently announced the creation of the VoIP Security Alliance (www.voipsa.org) focusing on all aspects of VoIP security. An article outlining the VoIP Security Alliance can be found at http://www.securitypipeline.com/showArticle.jhtml?articleID=59301706.

The industry press increasingly contains articles discussing VoIP security. One example would be the MierCom test between two major VoIP vendors done for a Network World Fusion article. This offers insight to the vendor's perspective on VoIP security as well as demonstrating differing security approaches, their ease and or difficult.
(http://www.nwfusion.com/reviews/2004/0524voipsecurity.html).

Additionally more standards bodies have taken to investigating, discussing and publishing VoIP security related information. An excellent compilation on the many aspects and issues faced by those attempting to secure VoIP is the National Institute of Standards and Technology recently published Special Publication 800-58 "Security considerations for Voice over IP systems" by authors D. Richard Kuhn, Thomas J. Walsh and Steffen Fries (http://www.nist.gov/).

It's important to note that the ITU has recognized the need for security in H.323 and has published the H.235 version 3 "Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals". In brief H.235v3 recommends methods by which terminals can authenticate and establish encrypted communications via H.245 exchanges. H.235v3 may or may not be implemented by the H.323 vendor. The ITU is continually investigating methods to improve H.323's security.

Future Considerations

VoIP deployments will inevitably continue until the technology is as accepted, expected and known in the network as any other IP technology. Whether H.323, SIP or some yet to be developed protocol it will need to be understood, protected and incorporated into security architectures. Two areas for improvement have been identified within this document to increase H.323's security and interoperability with existing network vendor equipment.

Too often in the H.323 Operation section the phrase "vendor specific" is used to describe the communication ports used for connectivity within H.323 (other than 1719,

1720). Improving security would require the proper organizations (ITU, IETF and IANA) to reach agreement with VoIP vendors to assign specific port numbers or ranges of port numbers to be used in H.323 communications. It is time to re-evaluate the current well known port assignments in TCP/UDP to include more of this growing service. This will ease deployment programming, reducing complexity and increase security as businesses communicate using different vendor's VoIP equipment. Firewall rules can then be made more specific, narrowing the ports needed, providing increased security with minimum impact to interoperability. This definitely must be a point of discussion and addressed as we move toward more IP version 6 (IPv6) deployments.

The second security improvement is from Firewall equipment vendors. Today's stateful firewalls recognize H.323's port 1720 flows but most (any?) do not associate the later RTP media stream setup initiated by it. The VoIP vendor's ports are (usually) simply known and open in the firewall to allow this communication to be established. Unfortunately these UDP port numbers, above 1024, are also used by viruses, Trojan's and spyware. Firewall vendors should expand their stateful firewall code and processes to include the expected RTP media stream setup with that of the well known port 1720 to increase and improve security.

In closing, the recommendations within this paper provide a starting point for addressing the security requirements of an H.323 network. The recommendations can be reviewed before deployment or applied to an existing network. With training and planning this can be accomplished with minimum effort and cost compared to the benefits gained. Many of the recommendations will be familiar to security professionals but then VoIP is in essence an application over IP with its own unique parameters and operation that needs to be secured.

References:

H323

http://www.dialupaudio.com/h323primer.html

http://www.openh323.org/

http://www.h323forum.org/

www.itu.org

www.ietf.org

Vulnerabilities

http://www.cert.org/nav/index_red.html

http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/h2250v4/index.html

http://www.securityfocus.com/bid

Other sites of interest (VoIP and/or Security)

www.voipsa.org

http://www.nist.gov/

http://www.voip-info.org/tiki-index.php

http://www.packetizer.com/

Assignment 2: Security Architecture

GIAC Enterprises is a small business which markets fortune cookie sayings to customers worldwide. GIAC employs fifty people with the majority located in or near its head office and the remainder located in or near the four regional satellite offices geographically distributed around the world. All of GIAC Enterprise sales are done via the Internet. GIAC Enterprises is investigating improvements to the current security architecture. As a small business the solution must provide a balance between security and cost. GIAC Enterprises emphasized cost control as a priority in the proposed solution. The solution must address the security concerns of several types of customers each requiring different methods of, and levels, of security. This document describes the security recommendations for GIAC Enterprises. The proposed solution provides cost effective security for all aspects of GIAC Enterprises business needs.

Access Requirements

It is recommended that GIAC Enterprises deploy several secure access methods to cost effectively provide the security necessary for business.

Customers

GIAC Enterprises is a global business supplying customers from around the globe. Potential customers will require access to the GIAC website. Customers requiring purchases will require secure access for their orders and transactions to the GIAC web server. Customers will accomplish this via HTTPS.

Suppliers

GIAC Enterprises prides itself on providing a superior product at the lowest cost to its customers. GIAC buyers are constantly searching for suppliers that can provide the best prices for its business needs. GIAC purchasing agents will need HTTP and HTTPS access from the corporate network to supplier websites.

Partners

Partners are determined by GIAC Management. Partners require access to the GIAC MS-SQL servers to check order status and access the server translation service. Partner access is permitted into the GIAC corporate network to these servers. Partner access will be provided by IPSec VPN tunnels.

Employees

GIAC employees on the corporate network will require outbound web access while maintaining protection from unauthorized intrusions and threats. GIAC Enterprises has several remote locations with employees. IPSec VPN's will be used for secure interconnectivity between corporate locations. The current ip address scheme (non-routable, RFC1918) will be maintained. GIAC employee access to web sites and

internet services will be provided via NAT. GIAC EMAIL service will maintain current connectivity, to an external provider, with a direct one to one ip address mapping and firewall policy. DNS functions for internet access will be provided by the firewall.

Sales/Teleworkers

GIAC employs a small but dedicated sales department which travels extensively in support of customers, partners and trade shows. Each Sales representative will deploy VPN client software for secure connectivity back to the GIAC Enterprises sites. GIAC Teleworkers will deploy the same connectivity scenario. Wherever Teleworkers and the Sales Force have access to broadband internet connections they will be capable of connecting into the GIAC corporate network.

General Public

Access must be provided to the general public to the GIAC online catalog. This will continue to be provided, as today, via internet access to the GIAC Web Server behind the new firewall.

Data Flows

Below is an example of the expected data/call flows necessary to be secured for GIAC Enterprises.

Source	Destination	Port(s)/Protocol	Description
General Public / Potential Customers	GIAC Web Server (internal)	80/TCP (HTTP)	Web access for general public browsing of the online catalog. Netscreen MIP function to appear as 65.97.168.253 to internet
Partner	Partner VPN Server	500/UDP (IKE)	IKE Permits key negotiation for establishment of the VPN.
Partner	Partner VPN Server	IP 50 (ESP)	Partner VPN Access to permit downloading of fortunes
Partner VPN	Partner Database Server	1433/TCP (MS-SQL)	Partner access to database server via SQL Client. Permits partner to access to the fortunes database to download for translation.
Sales Force / Teleworkers	Corporate email servers and services	500/UDP (IKE) IP 50 (ESP IPSec)	Permits Sales and Teleworkers secure access to GIAC Enterprises corporate email services from remote locations.
GIAC Enterprises remote offices	Corporate LAN, servers and services	500/UDP (IKE) IP50 (ESP IPSec) (ALL)	Provides secure communications and sharing of corporate resources between remote corporate offices.

GIAC Employees	Internet access	(80) HTTP (443) HTTPS NAT	Generic HTTP Internet access via NAT Secure HTTP Internet access to secure connection to remote supplier websites
Corporate Email	Internet Provider	SMTP (25)	GIAC Corporate email server and services. Netscreen MIP function to appear as 65.97.168.254 to internet
DNS	Internet Provider	DNS (53)	Domain Name Service in support of internet access provided by Netscreen 5GT.

Architecture Components

The below section details the operation components and their functions to be deployed in the GIAC Enterprises secure network architecture.

Filtering Router(s)

The GIAC Enterprises existing internet router will be re-used. The configuration will be modified to improve security with the addition of "access-lists" on the egress ethernet interface connecting to the GIAC Firewall. In addition secondary IP addresses will be configured for use in the new VPN tunnel configuration (Corporate Remote, Partners and Teleworkers). The existing router is a Cisco 4000 IOS version 12.0. Details of the configuration additions (access-lists) are describe in a later section.

Firewall(s)

A Netscreen 5GT (screenOS 5.1.0z) will be installed providing the primary access point, firewall functions and VPN Tunnel termination for the GIAC network. The Netscreen 5GT provides the necessary interfaces, firewall policies and VPN capabilities for the proposed GIAC security architecture.
The Netscreen will provide NAT translation for the private network addressing scheme currently in use by GIAC Enterprises to allow GIAC users Internet access.
The Firewall will provide a "mapped ip" function (MIP) for the GIAC corporate Email server and the GIAC catalog Webserver. This function will provide constant one-to-one public-private address translation for these two devices. The GIAC Website will always be connected to and represented as IP address 65.97.168.253 and the GIAC corporate email server will always be connected to and represented as 65.97.168.254 by external sources.
The Firewall provides DNS resolution for GIAC users needing access to the internet. The Firewall has been configured with the Primary ISP DNS address of 65.97.168.5 and secondary address DNS address of 64.97.168.5.

Webserver

The GIAC Webserver will be located behind the GIAC corporate firewall with a hard coded private IP address of 192.168.1.254. The Firewall's MIP functionality will provide a one-to-one NAT translation to 65.97.168.253. This IP address (65.97.168.253) will be the IP address presented to the internet as the IP address of the GIAC Webserver.

Policies will be configured in the Firewall allowing only HTTP and HTTPS connectivity from the Internet to/from the GIAC Webserver.

VPN(s)

The Netscreen 5GT will be configured to meet the firewall criteria and act as the VPN tunnel appliance. After review of GIAC Enterprises access requirements it is recommended that three (3) individual and separate VPN termination points be configured and deployed to increase security. Each remote VPN required is offered additional security by termination to a separate IP address on the Netscreen 5GT (secondary IP addresses). This is accomplished by utilizing IP addresses in the public IP address space provided by the Internet Service Provider (ISP) on the Netscreen and the network boarder router. They VPN tunnel/termination requirements are as follows:

Remote Offices - Route-based VPN's (LAN to LAN)
Partners - Policy-based VPN's (LAN to LAN)
Teleworkers - VPN client (LAN to LAN)

Remote Offices
VPN access is provided to/from GIAC remote corporate offices to the MAIN corporate location. Each remote site has its' own VPN tunnel back to the MAIN site and configured as 'route-based' VPN's. Remote corporate office LAN's are allowed access to all services and servers at the MAIN corporate site. There is no VPN security policy (permit ALL) as per instructions from GIAC management to allow full and complete access between corporate sites. This simplifies policy rules and eases equipment processing demands. Remote offices will use a private address range (192.168.x.x) for their local subnets, the VPN routed tunnels allowing connectivity between these and the corporate subnet of 192.168.1.0. The assignment of Remote Office subnets is listed in the GIAC Network IP Address Assignment sheet.

Partners
A separate VPN tunnel is provided for each of the three (3) remote Partners. Partner VPN access and the associated policy allows access to only those servers and services necessary and described by GIAC Network Operations. VPN security policy's have been configured and assigned to each Partner VPN tunnel. As per prior discussions the VPN security policy has been defined allowing access to/from Partners only to the server (192.168.1.248) and services (MS-SQL-S) discussed and determined as necessary by GIAC management. Partners have been instructed to use the private address range of 172.16.x.x for their devices requiring connection to the GIAC SQL servers. The assignment of Partner private ip subnets is listed in the GIAC Network IP Address Assignment sheet.

Teleworkers
Remote workers and the Sales force will be provided a separate VPN termination for access to only the GIAC email server and services. VPN clients will be installed and configured on each users PC expected to require this access. Teleworkers once

connected will be restricted to GIAC email server and services. Teleworker access is locally provided by any broadband internet access available.

Network based IDS sensor

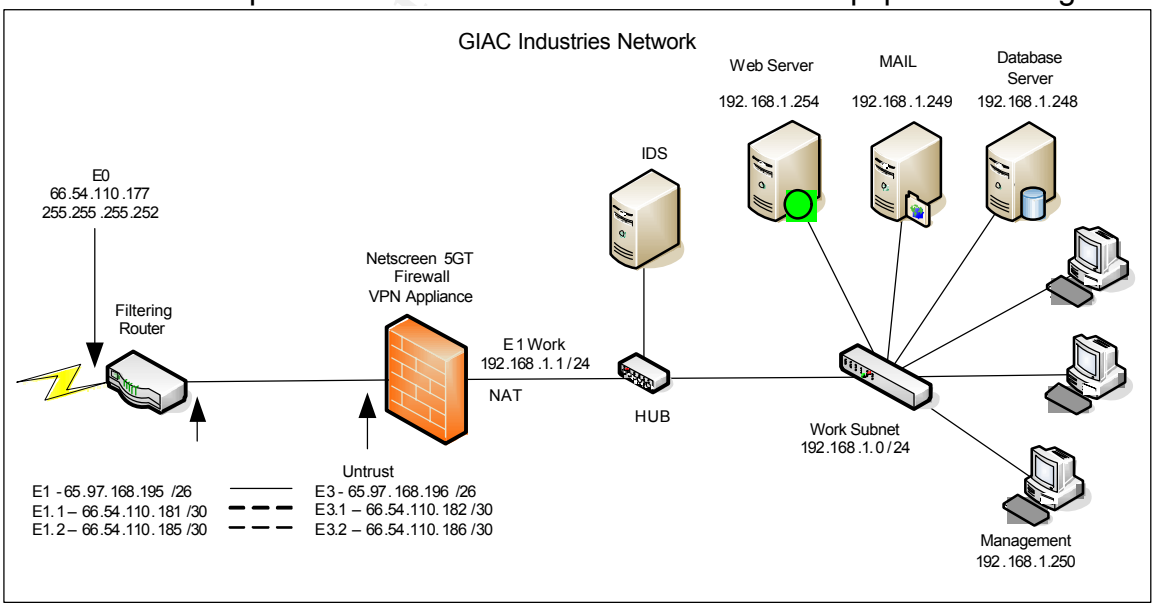
A Network based Intrusion Detection System will be installed to provide monitoring, logging and alerting for abnormal, invasive and potentially destructive traffic flows into the GIAC Enterprises network. The McAfee IntruShield 1200 (I-1200) was selected for the deployment. The unit offers the cost / performance required and should prove easy to use and maintain by GIAC's existing Network Support personnel. With additional training GIAC Network Support can enable advanced functionality to further enhance network and Webserver security. The N-IDS will be pre-configured with the manufacturer's database as well as be updated on a regular and as needed basis. A one year maintenance and support contract (McAfee PrimeSupport) is recommended.

Additional Components – EMAIL

GIAC Enterprises requested coordination and security configuration for connectivity between the internal EMAIL server and an externally provided EMAIL service. This was provided by the MIP function in the Firewall for direct one to one mapping of the internal EMAIL server IP address (192.168.1.249) to an available public IP address (65.97.168.254) which is an Internet routable host address available to GIAC. The Netscreen 5GT will provide this via the MIP function on ethernet port 3 (Untrusted). Teleworkers will only be allowed access to corporate email services when connected.

Network Diagram

The below network diagram represents the proposed components and layout of the security / network architecture proposed at the MAIN GIAC Enterprises corporate location. GIAC Enterprises remote offices will have a similar equipment arrangement.



IP addressing scheme

IP addressing of components used and assigned throughout the network is detailed below as well as with a diagram on the next page. This is a reference for the GIAC MAIN site only. GIAC Enterprises has been provided a block of public ip address by their Internet provider (subnet = 65.97.168.192 / Mask = 255.255.255.192)

Netscreen 5GT interface e1 (work) 192.168.1.1

Default router interface for all Servers and PC's on Main corporate LAN. The Netscreen provides NAT (to the E3 interface IP address of 65.97.168.196) for this subnet to allow Internet connectivity.

Netscreen 5GT interface e3 (Untrust) 65.97.168.196 / 255.255.255.192

Internet access interface with public IP address. This interface and its subnet are used as the NAT address for the 192.168.1.0 network "Work" LAN. This interface is also used as the GIAC remote corporate site IPSec tunnel origination / termination interface.

Netscreen 5GT interface e3.1 (Untrust) 66.54.110.181 / 255.255.255.252

Secondary Internet access interface with public IP address used as origination / termination address for Partner IPSec tunnel termination.

Netscreen 5GT interface e3.2 (Untrust) 66.54.110.186 / 255.255.255.252

Secondary Internet access interface with public IP address used as origination / termination address for Teleworkers IPSec tunnel termination.

Cisco router

Default router for GIAC Enterprises connectivity to the Internet provided by the ISP.

Cisco router interface e0

Internet access interface with public ip address 66.54.110.177 providing a direct connection to Internet provider's (ISP) network.

Cisco router interface e1 - 65.97.168.195 /26

Main IP address assignment for the GIAC public network (internet). This ip address range also provides the termination address for the IPSec VPN tunnels to GIAC remote corporate office (regional offices).

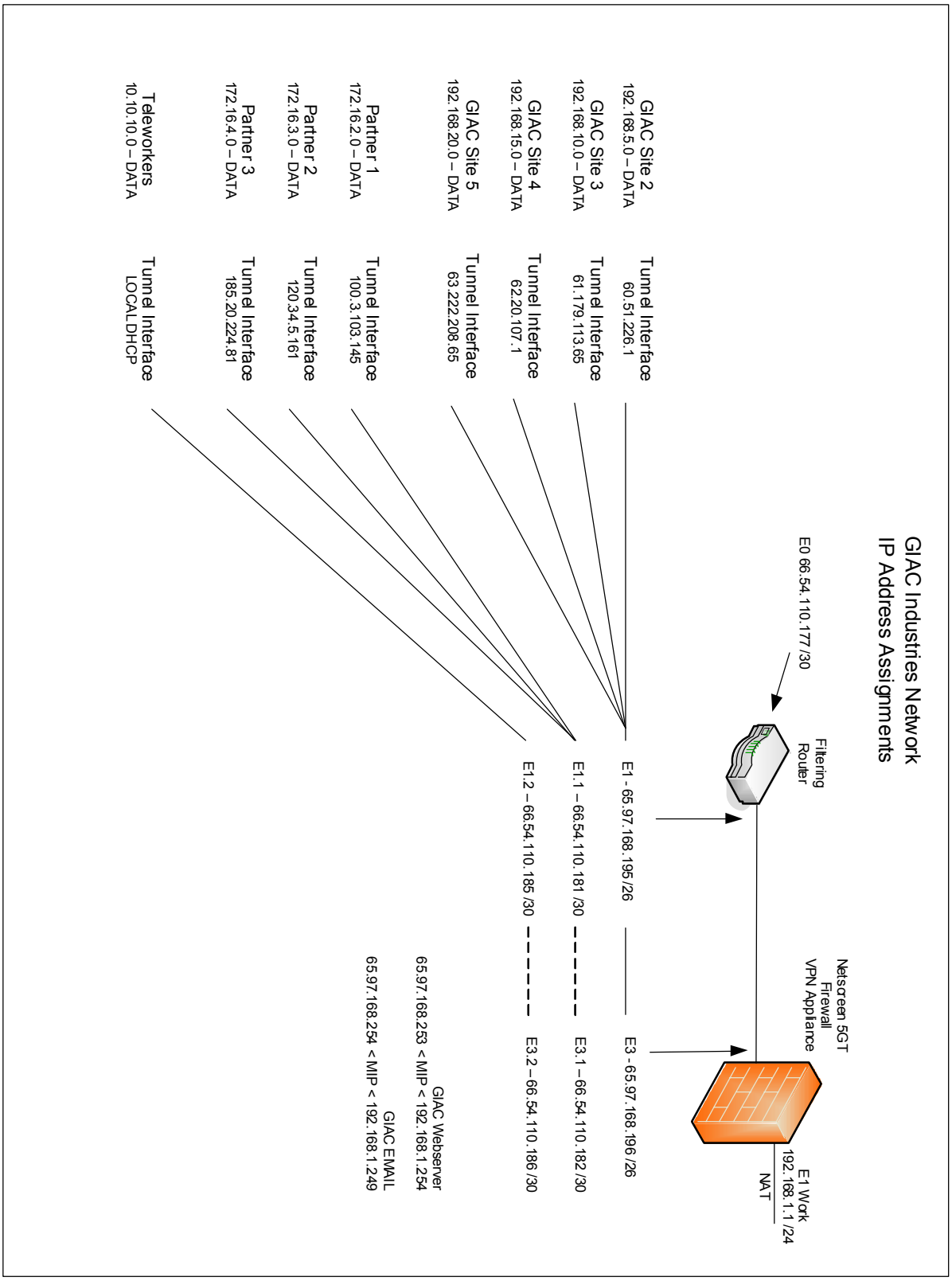
Cisco router interface e.1.1 - 66.54.110.181 /30

Secondary ip address to provide ip address for tunnel termination from remote Partners in conjunction with GIAC VPN Appliance (Netscreen 5GT)

Cisco router interface e.1.2 - 66.54.110.185 /30

Secondary ip address to provide ip address for tunnel termination from remote Teleworkers in conjunction with GIAC VPN Appliance (Netscreen 5GT)

GIAC Enterprises Network IP Address assignments.



Implementing Defense in Depth

It is our policy to design and propose "defense in depth" systems for all our potential customers. Defense in depth is engineering to provide a variety of security mechanisms at a variety of points throughout the network determined by the connectivity needs. Each component provides a measure of traffic isolation, monitoring and or screening before the next component. The proposed solution provides defense in depth by use of the following methods.

Filtering Router
The existing internet router, Cisco 4000 IOS version 12.0, will be used with the addition of access lists to improve security. The access-list is applied to the egress interface (connected to the GAIC network) of the router. The access lists will allow only the traffic determined as necessary to the Firewall and entry into the GIAC network.

Secondary IP Addresses
Secondary IP addresses are configured on the router egress interface and the ingress interface of the GIAC firewall. These subnets and their addresses provide individual and unique addresses for the IPSec tunnel terminations recommended. Secondary IP addresses are not "ping-able" and provide protection against ICMP probing and reconnaissance attempts.

IPSec VPN Tunnels
Traffic security between GIAC Enterprises sites, Partners and Teleworkers is provided by IPSec VPN Tunnels. Each GIAC location, Partner or Teleworker group is provided an individual tunnel interface and associated policy. The VPN tunnels provide encryption of sensitive traffic across the internet between corporate and Partner locations. In additional the tunnels provide obscurity of the actual ip addresses in use at the terminating locations by using ESP. The IPSec VPN tunnel appliance used at all GIAC Enterprises sites is the Netscreen 5GT.

Firewall
A Netscreen 5GT (screenOS 5.1.0z) will be deployed to provide the firewall function at all GIAC Enterprises locations. The Firewall is configured with several policies allowing only that traffic determined as necessary by earlier interviews with GIAC Management. In addition as the entrance to the GIAC network the firewall provides protection through the "Screening" configuration option to recognize and prevent numerous well known penetration and denial of service attacks. The firewall configuration and policies provide traffic isolation and separation between the GIAC network, Partners, Teleworkers and general Internet access of the GIAC Enterprises employees.

NAT (Network Address Translation)
GIAC Enterprises PC's and Servers are programmed with non-routable IP address in the 192.168.1.0 subnet range. GIAC's Internet provider supplied a block of routable IP addresses for use in the 65.97.168.192 subnet range. The Netscreen 5GT Firewall will provide NAT from non-routable to routable addresses allowing all necessary Internet access. The NAT programming and translation will obscure the ip address

assignments within the network making them less vulnerable to network scanning.

N-IDS (Network - Intrusion Detection System)
The N-IDS will provide monitoring, logging and alerting for abnormal, invasive and potentially destructive traffic flows within the GIAC Enterprises network. The N-IDS will be pre-configured with the manufacturers default database as well as be updated on a regular and as needed basis. Connectivity to the GIAC network will be located between the layer 2 switch (which all GIAC Servers and PC's connect to) and the Netscreen 5GT Firewall. The physical connectivity will be by a layer 2 shared HUB, the N-IDS system NIC card placed in promiscuous mode. The N-IDS is positioned to monitor all traffic allowed in/out from the Firewall to the GIAC Webserver, Partner server and user network.

Additional Defenses
In addition to the firewall policies the Netscreen 5GT provides the ability to recognize, control and/or prevent a variety of well known attacks and vulnerabilities. This is available through the "Screening" option and has been configured and enabled to provide increased protection for the GIAC corporate network. Detail of the additional protection is provided at the end of Assignment 3 under "Additional Defenses".

It is our policy to design and propose "defense in depth" systems for all our existing and potential customers. The benefits and shortcomings are thoroughly presented and discussed throughout all levels of the client organization. A variety of options ranging in cost / benefit are discussed and presented. This was the case with GIAC Enterprises. As an internet based small business GIAC Enterprises understands the need for security and protection of their assets, customers and reputation. The cost of the solution is a primary concern as well as any ongoing maintenance and support. The solution and components presented represent an excellent balance of security, functionality and cost.

Assignment 3: Router and Firewall Policies

The below documentation details the access-list policies of the Border router (previously designated Filter Router) and the Netscreen Firewall / VPN Appliance used in the GIAC Enterprises network.

General Security Stance

The general security stance is to provide an effective defense in depth within the customers established cost objectives.

Border Router(s) Security Policy

The updated access-list configuration for the Cisco 4000 is listed below. The new access-list configuration is designed to filter traffic and protocols from the Internet and allow only those necessary for the business of GIAC Enterprises. The access-list is applied as an egress list to router port e1. The access-list has been designed and configured to minimize processing overhead in the router – the traffic types listed in expected volume order.

```
access-list 101 permit tcp any host 65.97.168.253 eq www
access-list 101 permit tcp any host 65.97.168.253 eq 443
access-list 101 permit esp any any
access-list 101 permit udp any any eq isakmp
access-list 101 permit tcp host 63.97.168.254 host 65.97.168.254 eq smtp
access-list 101 permit ip any host 65.97.168.196
access-list 101 deny   ip any any
```

These access statements permit any HTTP and HTTPS traffic to the GIAC Webserver IP address.

```
access-list 101 permit tcp any host 65.97.168.253 eq www
access-list 101 permit tcp any host 65.97.168.253 eq 443
```

This access statement permits any ESP traffic to the GIAC site.

```
access-list 101 permit esp any any
```

This access statement permits any isakmp traffic to the GIAC site.

```
access-list 101 permit udp any any eq isakmp
```

This access statement permits traffic between the Internet Email server to the GIAC Email server IP address.

```
access-list 101 permit tcp host 63.97.168.254 host 65.97.168.254 eq smtp
```

This access statement permits any IP traffic to the GIAC Firewall (which performs addition policy filtering).

```
access-list 101 permit ip any host 65.97.168.196
```

The final statement is an explicit “deny any”.

```
access-list 101 deny   ip any any
```

Primary Firewall(s) Security Policy

This documentation details the firewall policies of the Netscreen 5GT installed at the GIAC Enterprises MAIN site. The policy configuration is designed to filter traffic and protocols from the Internet and allow only those necessary for the business of GIAC Enterprises. The policies have been designed and configured to minimize processing overhead – the traffic types listed in expected volume order. The "ICMP-ANY" policy will be removed after installation testing. Logging has been enabled for all policies.

Outbound Policies

The firewall policies are referred to by the interface names and direction they apply to "Work to Untrust" and "Untrust to work". The "Work" interface refers to ethernet e1 with IP address 192.168.1.1 /24. The "Untrust" interface refers to ethernet e3 with IP address 65.97.168.196.

Firewall Policies for Work to Untrust

From Work To Untrust, total policy: 7

ID	Source	Destination	Service	Action	Options	Configure			Enable	Move
26	Any	Any	HTTP HTTPS			Edit	Clone	Remove		
13	192.168.1.248/32	Partner1	ICMP-ANY MS-SQL-partners			Edit	Clone	Remove		
14	192.168.1.248/32	Partner2	ICMP-ANY MS-SQL-partners			Edit	Clone	Remove		
15	192.168.1.248/32	Partner3	ICMP-ANY MS-SQL-partners			Edit	Clone	Remove		
23	GIAC-EMAIL	email-server	ICMP-ANY SMTP			Edit	Clone	Remove		
29	GIAC-EMAIL	Teleworker	SMTP			Edit	Clone	Remove		

Policy ID 26 allows any corporate user to access any internet web servers / websites with only HTTP and HTTPS. NAT is provided on interface e1 "Work" to the primary ip address of interface e3 (65.97.168.196) on the Netscreen 5GT.

Policy ID's 13, 14 and 15 allow outbound traffic from the database server (192.168.1.248) to the Partner VPN tunnels and Partners. This traffic is restricted to MS-SQL traffic, a custom defined service for tcp port 1433.

Policy ID 23 allows only corporate email to ISP email server communications with

SMTP. The corporate email server is 'MIP' to ip address 65.97.168.254.

Policy ID 29 allows corporate email connection and services to Teleworkers when Teleworkers are properly authorized and connected via the dynamic Teleworker VPN connection.

Inbound Policies

The firewall policies are referred to by the interface names and direction they apply to "Work to Untrust" and "Untrust to work". The "Work" interface refers to ethernet e1 with IP address 192.168.1.1 /24. The "Untrust" interface refers to ethernet e3 with IP address 65.97.168.196.

Firewall Policies for Untrust to Work

From Untrust To Work, total policy: 5

ID	Source	Destination	Service	Action	Options	Configure			Enable	Move
25	Any	Webserver	HTTP HTTPS			Edit	Clone	Remove	☑	
16	Partner1	192.168.1.248/32	ICMP-ANY MS-SQL- partners			Edit	Clone	Remove	☑	
17	Partner2	192.168.1.248/32	ICMP-ANY MS-SQL- partners			Edit	Clone	Remove	☑	
18	Partner3	192.168.1.248/32	ICMP-ANY MS-SQL- partners			Edit	Clone	Remove	☑	
28	Teleworker	GIAC-EMAIL	SMTP			Edit	Clone	Remove	☑	

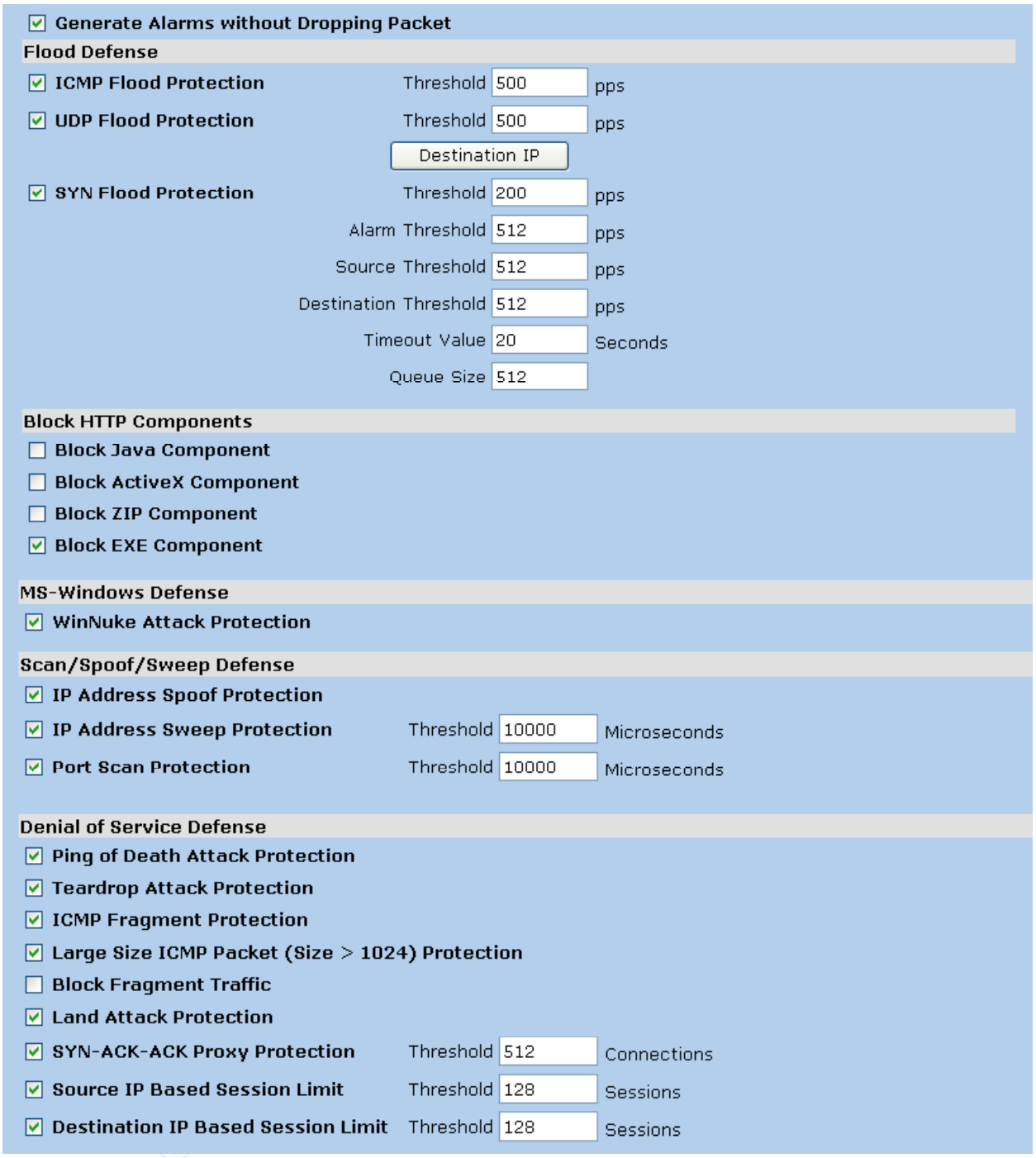
Policy ID 25 allows any HTTP and HTTPS into the network only to the GIAC Webserver.

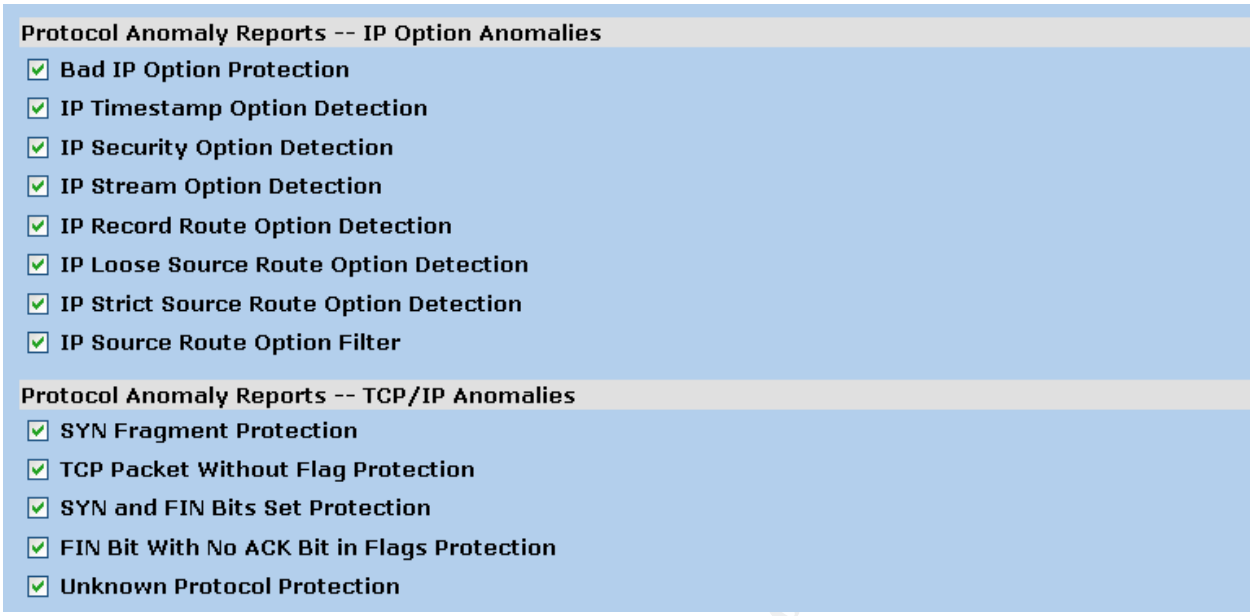
Policy ID's 16, 17 and 18 allow inbound traffic from the Partners sites and VPN tunnels only to the database server (192.168.1.248). This traffic is restricted to MS-SQL traffic, a custom defined service for tcp port 1433.

Policy ID 28 allows Teleworkers access to the corporate email services after Teleworkers are properly authorized and connected via the dynamic Teleworker VPN connection.

Additional Defenses

In addition to the firewall policies the Netscreen 5GT provides the ability to recognize, control and/or prevent a variety of well known attacks and vulnerabilities. This is available through the "Screening" option and has been configured and enabled to provide increased protection for the GIAC corporate network.





References

Netscreen Product Documentation CDROM

Configuring Netscreen Firewalls
Syngress Publishing, Inc.
ISBN 1-932266-39-9

CCSP Self Study: Cisco Secure PIX Firewall Advanced (CSPFA)
Cisco Press
ISBN 1-58705-149-4