RADVISION Firewall

Cookbook

NOTICE

Firewall Cookbook version 1.0, January, 2002

Publication 1

http://www.radvision.com

DISCLAIMER

The information in this document is provided in good faith but without any representation or warranty whatsoever, whether it is accurate, or complete or otherwise and on the express understanding that RADVISION shall have no liability whatsoever to other parties in any way arising from or relating to the information or its use.

CONTENTS

About This Manual

The RADVISION Firewall Cookbook describes solutions for H.323 communication through firewalls and NATs.

The Firewall Cookbook currently describes three alternative solution types:

- H.323-aware firewalls
- H.323 Proxies
- Traversal solutions

For each alternative, the Firewall Cookbook provides

- A short description of the nature of the solution.
- An indication of the suitability of the solution (for example, for SOHO, Service Providers or enterprises).
- A description of the configuration and topology of the solution.
- An explanation of how the solution works.
- How the solution integrates with RADVISION devices.
- Links for more information.

Version 1 of the Firewall Cookbook includes solutions from the following companies (in alphabetical order):

- Cisco
- NetScreen
- Ridgeway

There are a variety of other solutions. As we gather more information, we will update the Firewall Cookbook to reflect new and updated solutions.

Note The information in this manual comes from a variety of sources and has not necessarily undergone all the usual RADVISION interoperability procedures.

1

INTRODUCTION

ABOUT THIS COOKBOOK

This Firewall Cookbook describes how to provide secure communication for voice and video data over packet networks and describes a selection of solutions and the issues they raise. The Firewall Cookbook is intended for users who wish to conduct secure voice and/or video conferences by integrating their RADVISION devices with their existing (or soon to be acquired) firewalls and/or NATs.

WHAT ARE FIREWALLS?

A firewall is a barrier device placed between two separate networks. There are two popular types of firewalls:

- Packet Filters that block traffic by applying filtering rules based on IP addresses and/or port numbers. A Packet Filter makes security decisions such as “forward this packet” or “don’t forward this packet”.
- Application Level Gateways (ALGs) serve as communicators between two networks. ALGs are protocol-aware entities that examine application protocol flows and only allow messages that conform to security policies to pass.

Sometimes ALGs are erroneously referred to as *Proxies*. There is a difference between the two. ALGs are transparent to the multimedia entities but Proxies are not. Proxies are an integral part of the multimedia system. For example, for H.323 the Proxy would be a gatekeeper (most probably with basic or limited functionality) while for SIP it would be a specialized SIP Proxy.

A firewall can be implemented in a single router that filters out unwanted packets or it can use a variety of technologies in a combination of routers and hosts. In the latter, network administrators centrally define and maintain the restriction policies. Today many firewalls combine filtering functionality with NAT functions.

WHAT ARE NATS?

Network Address Translation devices (NATs) translate IP addresses so that users on a private network can see the public network, but public network users cannot see the private network users. Typically, on outgoing packets a NAT device maps local private network addresses to one or more global public IP addresses. On incoming packets the NAT device maps global IP addresses back into local IP addresses.

There are two types of NAT devices:

- A NAT device that allows an organization to use a range of private IP addresses when communicating within an inside network and to share a small pool of public IP addresses when communicating with an outside network.
- A Network Address Port Translator (NAPT) or Port Address Translator (PAT) device that has a block of inside addresses and one or more outside addresses. The port number is the differentiator.

ABOUT VPN

Virtual Private Networks (VPN) technology is one of the approaches being used today for providing secure communications over IP networks. Virtual Private Routed Networks (VPRN), which ensures both security and QoS characteristics, is an attractive solution for Multimedia over IP communications.

VPN modules create closed secure tunnels for communication between two firewalled LANs. Firewalls and VPNs offer perimeter and access controls, but internal, remote or even authorized users can attempt to act against a company security policy. Once inside the VPN tunnel, firewalls cannot monitor authorized users' internal activities. Using VPN tunnels implicitly means that you are not traversing firewall rules and NATs.

There are three types of VPNs which align with how businesses and organizations use VPNs:

- Access VPN—Provides remote access to a corporate intranet or extranet over a shared infrastructure with the same policies as a private network. Access VPNs enable users to access corporate resources whenever, wherever, and however they require. Access VPNs encompass analog, dial, ISDN, Digital

Subscriber Line (DSL), mobile IP, and cable technologies to securely connect mobile users, telecommuters, or branch offices.

- Intranet VPN—Links corporate headquarters, remote offices, and branch offices over a shared infrastructure using dedicated connections. Businesses enjoy the same policies as a private network, including security, quality of service (QoS), manageability, and reliability.
- Extranet VPN—Links customers, suppliers, partners, or communities of interest to a corporate intranet over a shared infrastructure using dedicated connections. Businesses enjoy the same policies as a private network, including security, QoS, manageability, and reliability.

THE PROBLEM

The use of the H.323 protocol to send multimedia communication over IP has had unique consequences for firewall and NAT solutions. The problem consists of three specific issues:

- Call Setup and Signaling
- Traversal of Media Streams
- Deployment

CALL SETUP AND SIGNALING

Firewalls identify the source and destination IP address of a message, and allow or block the passage of the message according to the configured firewall policy. However, voice and video communications over IP use H.323 and other protocols. Messages sent with the H.323 protocol contain embedded transport addresses which the firewall cannot access.

Firewalls are configured with strict rules specifying static ports through which desirable data can pass while undesirable data is blocked. H.323 uses dynamically allocated port numbers. For example, an H.323 call typically requires a TCP connection for H.245 signaling and H.245 does not have a well-known port associated with it. The H.245 port is dynamic so it is clear that the firewall will block the H.245 message and the call signaling procedure will fail.

Similar issues affect NAT devices. For example, a SIP User Agent A, inside the network and behind a NAT, sends an INVITE message to User Agent B on the outside. In the simplest case, User Agent B extracts the From address from the INVITE message and sends a 200 (Ok) response to this address. Because the INVITE message came from User Agent A behind the NAT, the From address is “fictitious” (private) and incorrect. The 200 will not succeed and the call will not be connected.

Traversal of Media Streams

H.323 uses RTP for transporting the media streams. RTP runs over UDP and has no fixed ports associated with it. Each type of media stream has one or more channels but each channel requires its own pinhole to be opened. This means that for the media stream to traverse the firewall, the firewall needs to open many UDP pinholes for each call session, exposing the network behind the firewall.

Applying such pinholing does not solve the problem. Typically, the incoming and the outgoing media streams within the same multimedia session do not follow the same paths, in terms of UDP port numbers (and in some applications even in terms of IP addresses).

Furthermore, multimedia protocols do not necessarily know the source port of the media stream. This means that in some cases even application-aware Firewalls would not be able to dynamically open minimal tight pinholes.

Because of its connection-oriented nature, TCP has traditionally traversed firewalls more easily. Some of the solutions suggest traversing of media over TCP or/and using TCP tunneling. However, TCP has been designed for reliable streaming of large blocks of time insensitive information. Voice and video data is time sensitive (real-time) and relies on fast delivery of small unreliable packets. UDP is well suited for real-time media streams while using TCP for media streams results in poor voice and video quality.

Deployment

Firewalls and NATs are widely deployed in many types of environments, supporting a variety of topologies and serving a variety of users. Each type of environment, topology or user may require a different type of security solution. For example, where an MIS department of a large enterprise administers and controls the network and its security policies, a small home office typically has a few computers, uses an off-the-shelf NAT device and relies on an ISP for network services.

Further, legacy investment in firewalls and NATs, including the establishment of policies, results in a reluctance to change or upgrade hardware devices and/or security policies.

Existing Solutions

The following sections present three kinds of solution to the problem:

- H.323-aware firewalls
- H.323 Proxies
- Traversal solutions

For more information on H.323 solutions, see the RADVISION Technology White Paper *Traversal of IP Voice and Video Data through Firewalls and NATs*.

2

H.323-AWARE FIREWALLS

ABOUT H.323-AWARE FIREWALLS

H.323-aware firewalls provide application-level knowledge of the H.323 protocol. H.323-aware firewalls know how to access the IP address and port information of incoming or outgoing H.323 messages. An H.323-aware firewall examines every H.323 packet passing through it and blocks all unwanted communication attempts. Packets cannot enter a LAN unless they comply with company security policy. The H.323-aware firewall is transparent to multimedia entities.

Although some firewalls currently available on the market do support H.323 traversal, vendors do not all support the same or the latest version of H.323.

Some H.323-aware firewalls are capable of performing NAT functions together with the Multimedia over IP Protocols but there are currently no standalone ALG NATs in the market.

There are currently no SIP-aware firewalls on the market.

H.323-aware firewalls produced by Cisco and NetScreen are described below.

CISCO PIX AND IOS

The PIX firewall is a dedicated firewall appliance with its own hardware and operating system. The IOS firewall is integrated into the network through Cisco IOS software. The IOS software is available with a wide range of Cisco routers. The Cisco PIX firewall series and the Cisco IOS firewall both incorporate a range of features including:

- Stateful packet filtering
- IPSec VPN
- NAT

- Content filtering
- Redundancy/failover
- Intrusion Detection System

SUITABILITY

- The PIX firewall series is suitable for mass deployments with a large number of users.
- The IOS firewall is suitable for branch or remote office sites not requiring high performance.

CONFIGURATION

The PIX and IOS firewalls provide a single point of protection at the network perimeter. *Figure 2-1* illustrates a typical configuration using both these firewalls.

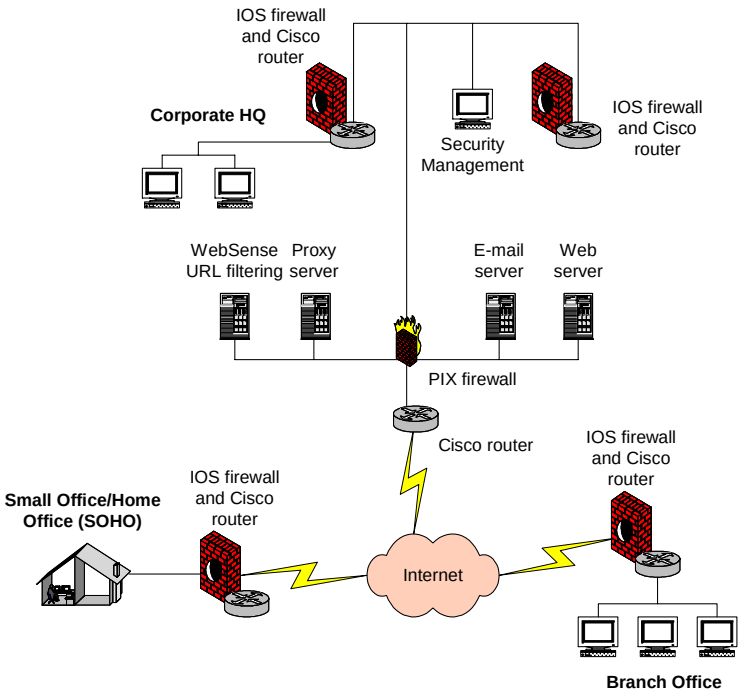

Figure 2-1 *Typical Configuration with PIX and IOS Firewalls*

HOW IT WORKS

Please refer to the appropriate vendor documentation.

Integrating RADVISION Devices

viaIP and OnLAN devices are transparent to users of Cisco firewalls.

Summary

Table 2-2 summarizes the security features that the Cisco PIX firewall series and the Cisco IOS firewall currently support.

Table 2-1 *PIX and IOS Security Features*

Calls Supported	Ports Activated	Addresses Rewritten in NAT
For specific information, consult the vendor.		

Link For More Information

For more information about Cisco or the PIX and IOS firewalls, see www.cisco.com.

NetScreen Security Solution

The NetScreen Next Generation Security Solution products combine firewall, VPN and traffic management on a single dedicated hardware platform. All of these products include an H.323-aware firewall and support IPSec VPNs.

H.323-aware Firewall

The NetScreen H.323-aware firewall has knowledge of the H.323 protocol so that it can extract, use or alter the embedded IP addresses and ports of incoming or outgoing data.

Note Only H.323 version 2 is currently supported.

Gatekeeper and MCU Routed Calls

The NetScreen H.323-aware firewall best supports Gatekeeper and MCU Routed calls when not in NAT mode. Any fixed ports needed in these cases should be opened by your company security policy.

The NetScreen H.323-aware firewall does not support scenarios requiring dynamically assigned ports to be opened (except in the RAS, Q.931, H.245 and RTP/RTCP cases described in the *Summary* section).

Gatekeeper and MCU Routed scenarios will fail when using NAT unless the call looks like a Direct Routed call to the firewall.

Future versions will offer support for Fast Start and H.245 Tunneling.

VPN

The NetScreen VPN offers a solution to the NAPT traversal problem based on a single manufacturer that provides an application that integrates the firewall, NAPT and VPN functions.

Note The NetScreen VPN solution only allows for communication among sites belonging to the same VPN, and does not allow for connectivity from and to end users or services located on a public network.

SUITABILITY

Enterprises.

CONFIGURATION

NetScreen Next Generation Security Solution is simple to configure:

- Set the gatekeeper to work in Direct Mode—no other special configuration of the gatekeeper is required.
- No special configuration of the gateway is required.

Figure 2-2 shows that gatekeeper devices can reside on either the trusted or untrusted side of a NetScreen device.

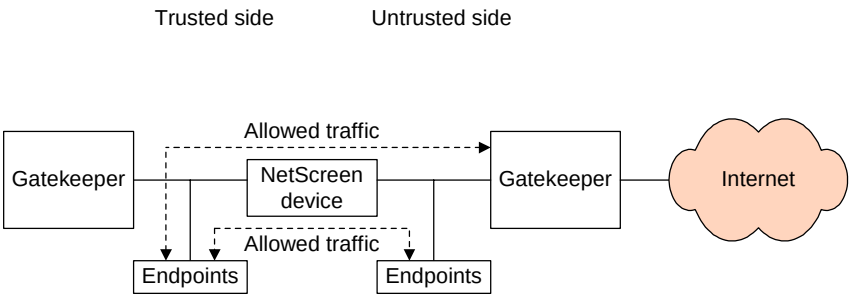

Figure 2-2 *General NetScreen Topology*

Trusted Gatekeeper (Transparent or Routed Mode)

In *Figure 2-3*, you set up two policies to allow H.323 traffic to pass between IP phone hosts and the gatekeeper on the trusted side and the IP phone at IP address 209.16.2.2 on the untrusted side of the NetScreen device, which can be in Transparent or Route mode.

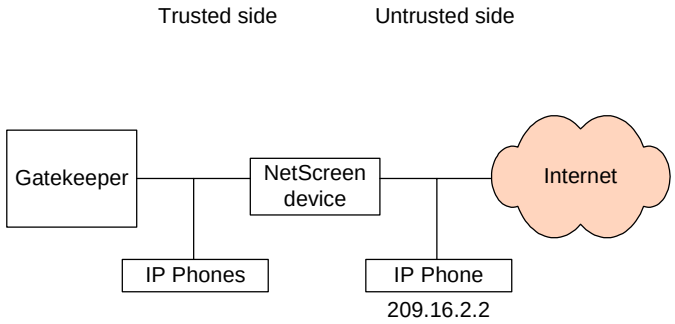

Figure 2-3 *Trusted Gatekeeper (Transparent or Routed Mode)*

Trusted Gatekeeper (NAT Mode)

When the NetScreen device is in NAT mode, a gatekeeper or endpoint device is said to be private when it resides on the trusted side, and public when it resides on the untrusted side. When you set a NetScreen device in NAT mode, you must map a public IP address to each private device.

In *Figure 2-4*, the trusted devices include the endpoint host (10.10.1.2) and the gatekeeper device (10.10.1.10). You configure the NetScreen device to allow traffic between the trusted endpoint host and gatekeeper and the untrusted endpoint host (210.10.1.2).

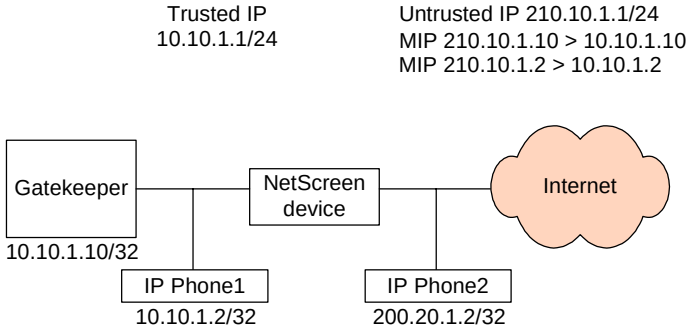

Figure 2-4 *Trusted Gatekeeper (NAT Mode)*

Untrusted Gatekeeper (Transparent or Routed Mode)

Because Transparent mode and Routed mode do not require address mapping of any kind, NetScreen device configuration for a gatekeeper on the untrusted side typically is identical to the configuration for a gatekeeper on the trusted side.

In *Figure 2-5*, you set up two policies to allow H.323 traffic to pass between IP phone hosts and the gatekeeper on the trusted side and the IP phone at IP address 209.16.2.2 on the untrusted side of the NetScreen device, which can be in Transparent or Route mode.

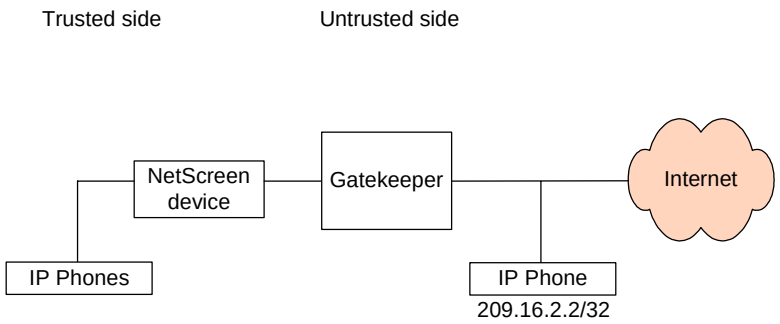

Figure 2-5 *Untrusted Gatekeeper (Transparent or Routed Mode)*

Untrusted Gatekeeper (NAT Mode)

In *Figure 2-6* the gatekeeper device (210.10.1.10) resides on the Untrusted side of the NetScreen device.

You configure the NetScreen device to allow traffic between the trusted host (IP Phone1) and the untrusted host (IP Phone2) and the untrusted gatekeeper.

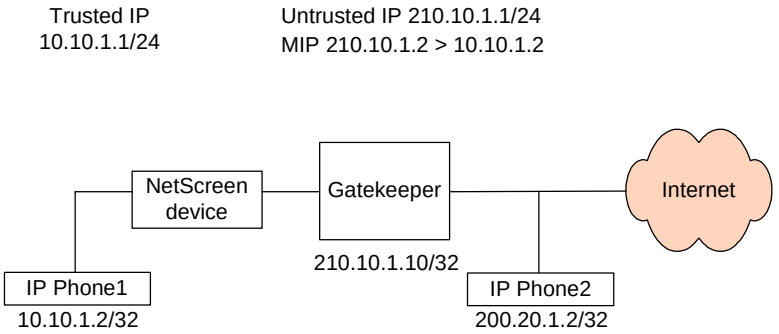

Figure 2-6 *Untrusted Gatekeeper (NAT Mode)*

How It Works

Please refer to the appropriate vendor documentation.

Integrating RADVISION Devices

viaIP and OnLAN devices are transparent to users of the NetScreen Next Generation Security Solution.

Summary

Table 2-2 summarizes the security features that the NetScreen Next Generation Security Solution currently supports.

Table 2-2 *Next Generation Security Features*

Calls Supported	Ports Activated	Addresses Rewritten in NAT
H.323 Direct and Gatekeeper Routed calls. H.225.0 RAS (except IRR messages).	TCP 1720 (Q.931) UDP 1719 (RAS) TCP 1503 (T.120)	Q.931 addresses. H.245 addresses. RAS messages (except for IRR which does not affect connectivity).

The NetScreen H.323-aware firewall inspects the traffic passing on TCP 1720 and dynamically opens a pinhole for H.245 traffic on the random TCP port chosen. The NetScreen H.323-aware firewall monitors this H.245 connection and opens the pinholes needed for RTP/RTCP.

Link For More Information

For more information about NetScreen or the NetScreen Next Generation Security Solution, see www.netscreen.com.

Check Point NG

The next edition of the Firewall Cookbook will describe the Check Point NG Firewall Solution.

3

H.323 PROXIES

ABOUT H.323 PROXIES

H.323 proxies are special types of gateways that relay H.323 calls to another H.323 endpoint. They can be used to isolate sections of an H.323 network for security purposes, to manage quality of service (QoS), or to perform special application-specific routing tasks.

H.323-compliant applications use dynamically allocated sockets for audio, video and data channels. To monitor and allow H.323 traffic through, a firewall must be either H.323-enabled with an H.323 proxy, or be able to check control channels to determine which dynamic sockets are in use for H.323 sessions, and allow traffic as long as the control channel is active.

4

TRAVERSAL SOLUTIONS

ABOUT TRAVERSAL SOLUTIONS

Traversal solutions traverse existing infrastructure and can realize connectivity without requiring modifications to firewalls and/or NATs as new protocols and revisions are introduced.

RIDGEWAY SECURE COMMUNICATOR V5.0

The Ridgeway® Secure Communicator™ v5.0 (vendor expected availability is in Q1 2002) enables enterprises and service providers to deploy secure services without infrastructure upgrades. The Secure Communicator also allows more open connectivity than VPN solutions. Furthermore, the Secure Communicator enables you to connect IP voice and video endpoints through your LAN, using your existing Internet connection and set up.

Note The Secure Communicator supports both the SIP and H.323 protocols.

Unlike H.323-aware firewalls, the Secure Communicator does not require upgrades to critical equipment and enables the administrator to define only a small set of rules that allow very few entities to communicate through very few ports.

The Secure Communicator contains two elements:

- A tunnel element for signalling and control information.
- A relay element for forwarding media without the overhead of true tunneling.

All voice and video communications pass through the Secure Communicator, other traffic takes its usual route. The two Secure Communicator components use only two well known ports, allowing firewall rules to be tight—the firewall

needs to allow connections between the two Secure Communicator components only. The firewall rules are thus simple and require no protocol awareness in the firewall. Furthermore, the NAT requires NO configuration. As a result, end users experience “plug and play” functionality and the behavior of the VoIP phone or conferencing device is unaffected.

SUITABILITY

SOHO and mobile deployments, Enterprises and Service Providers.

CONFIGURATION

The Secure Communicator is implemented as a pair of software components—the Secure Communicator Client (SCC) and the Secure Communicator Server (SCS).

Secure Communicator Client (SCC)

The SCC software resides within a private network space behind an enterprise or SOHO firewall. The SCC creates a signaling and control tunnel to the SCS beyond the firewall. Endpoints within the private space register with the SCC as if the SCC were a gatekeeper or SIP proxy. The SCC forwards all registration and call control traffic to the SCS, which relays the traffic to a service center gatekeeper or SIP proxy. The SCC also forwards media as required for calls. The SCC can be installed either on individual endpoints, or as a shared LAN resource to support multiple endpoints.

Remember! The SCC requires no special configuration of endpoints. Endpoints simply regard the SCC as a gatekeeper or SIP proxy and interact with it accordingly.

Secure Communicator Server (SCS)

The SCS software resides in the public space beyond the firewall. The SCS can be hosted by a service provider or hosted in an enterprise DMZ with enterprise mail and web proxies. The SCS acts as a proxy for a gatekeeper or SIP proxy in the service provider network or in the DMZ, as appropriate. All registrations and call signals received from an SCC are forwarded by the SCS to the service center gatekeeper or SIP proxy.

Remember! The gatekeeper or SIP proxy retains ultimate control of calls. The Secure Communicator acts as a transparent relay across intervening boundaries. Because the two components reside either side of your firewall, you do not need to upgrade the firewall.

Figure 4-1 illustrates a typical configuration using the Secure Communicator.

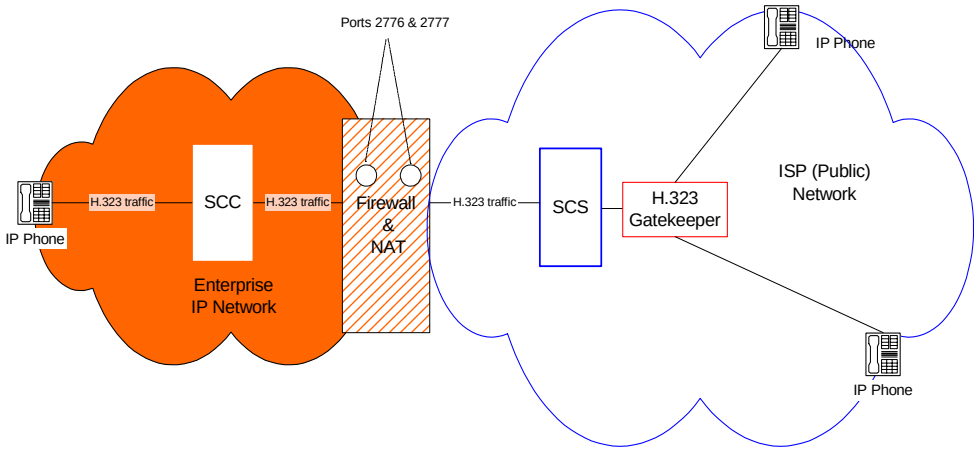

Figure 4-1 *Typical Configuration with Secure Communicator*

The SCC is deployed either at one of the endpoints that it supports or near the endpoints that it supports. The SCS can reside in the enterprise DMZ or at the service provider NOC/POP.

The SCS uses its IP stack to communicate effectively with other network communications equipment, including MCUs, firewalls, gateways, gatekeepers and so on. The system has two physical connections. One connection is used for management, and resides at the NOC DMZ or management network. The other NIC connection funnels all the voice and video traffic streams.

The Secure Communicator Server scales in a clustered model. Thus, several of these servers are able to coordinate in service delivery by neighboring. Additional servers can be added to a cluster at any time. Such a cluster is managed by a single management server. This management server also maintains a unified database for the cluster.

How It Works

Communication devices on the LAN regard the SCC as a gatekeeper or SIP proxy. LAN devices direct all registrations and outgoing calls to the SCC which relays the traffic to the SCS. Registrations and call control are sent through the tunnel to the two well known ports on the SCS. Media is forwarded over dynamic UDP connections to the well known ports on the SCS. The SCC and the SCS communicate via Ridgeway-licensed ports 2776 and 2777.

SCC authentication is by account number and PIN. The SCC must also know the IP address of its respective server. The SCC is blind to network set up, so it can exist in a DHCP or NAT environment. The SCC supports standards-based voice and video equipment (e.g. H.323 ViewStation, Vigo, PTel 970).

To set up the firewall for LAN-to-WAN calls

- Enable outbound and reply traffic to use ports 2776 and 2777 on the SCS.

LAN-to-WAN Call Procedure

1. The LAN user starts a call in the usual way using the endpoint interface.
2. The source endpoint sends a call request to the SCC.
3. The SCC tunnels the request through firewalls and NAT to the SCS which forwards it to the gatekeeper or SIP proxy.
4. The gatekeeper or SIP proxy response is relayed back to the source endpoint through the tunnel.
5. The source endpoint directs the call to the SCC.
6. The SCC relays the call to the SCS. The SCS forwards the call to the destination endpoint.
7. The destination endpoint gets call approval from the gatekeeper or SIP proxy and replies to the SCS. The SCS forwards the reply back through the SCC to the source endpoint.

Remember! The connection to the SCS uses a few well known ports.

Remember! The Secure Communicator conceals endpoint addresses by substituting its own. This ensures that all call traffic is routed through the Secure Communicator and that endpoint addresses remain private.

WAN-to-LAN Call Procedure

1. The WAN user starts a call in the usual way using the endpoint interface.
2. The source endpoint sends a call request to the gatekeeper or SIP proxy.
3. The gatekeeper or SIP proxy response indicates that the destination endpoint is the SCS.

4. The source endpoint directs the call to the SCS.
5. The SCS relays the call to the SCC.
6. The SCC forwards the call to the destination endpoint.
7. The destination endpoint seeks call approval from the SCC (as if the SCC were a gatekeeper or SIP proxy) and sends reply media to the SCC. Both communications are relayed from the SCC to the SCS and onwards as required.

Remember! The SCS amends the destination endpoint registration to substitute its own address, ensuring that WAN-to-LAN calls are routed to the SCS.

Remember! All channels are created outbound from the SCC regardless of the direction of media flow.

INTEGRATING RADVISION DEVICES

Figure 4-2 illustrates how to implement the Secure Communicator with viaIP.

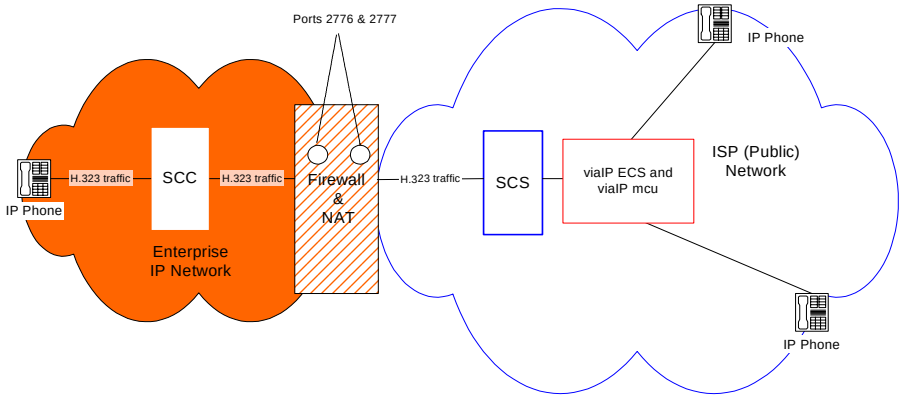

Figure 4-2 *Secure Communicator and viaIP*

SUMMARY

Table 4-1 summarizes the security features that the Ridgeway Secure Communicator currently supports.

Table 4-1 *Secure Communicator Security Features*

Calls Supported	Ports Activated	Addresses Rewritten in NAT
H.323 Direct and Gatekeeper Routed calls. H.323 RAS	UDP and TCP—Ridgeway well known ports 2776 and 2777. Ports 1719, 1720 and 1503 can be closed.	NAT translation is provided as required for all Q.931. H.245 and RAS messages. No reconfiguration of the NAST or configuration of the Secure Communicator is required.

The SIP solution is a call-stateful outbound proxy with NAT translations for all SIP messages as required.

SIP messages

- INVITE
- REGISTER
- ACK
- RESPONSE
- CANCEL
- SUBSCRIBE
- NOTIFY
- REFER
- INFO
- OPTIONS

The solution supports Supplementary Services such as Call Transfer.

LINK FOR MORE INFORMATION

For more information about Ridgeway or the Ridgeway Secure Communicator, see www.ridgewaysystems.com.