



Security and the Mitel Teleworker Solution

White Paper

Release 3.1

January 2005



White Paper

Copyright

Copyright © 2005 Mitel Networks Corporation. This document is unpublished and the following notice is affixed to protect Mitel Networks Corporation in the event of inadvertent publication: All rights reserved. No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of Mitel Networks Corporation. Trademarked Product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Table of Contents

INTRODUCTION	1
SOLUTION ARCHITECTURE	2
VOICE NETWORKING	5
RTP	5
Secure RTP	5
CAST-128	6
MAC Address Restriction	6
Resources	7
DATA SECURITY	8
Background on PPTP	8
Resources	9



White Paper

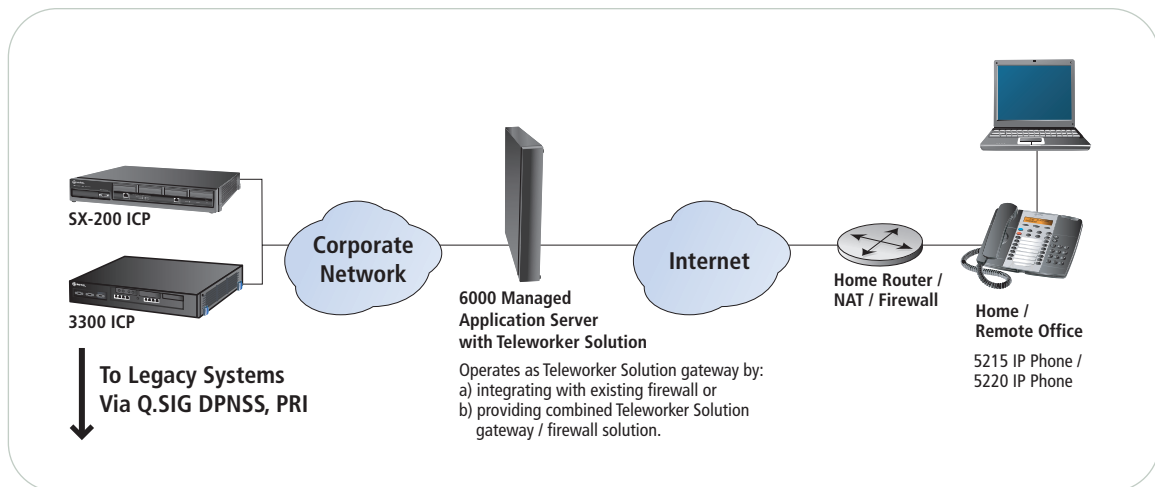
Introduction

The Mitel® Teleworker Solution enables remote workers to connect securely and conveniently to the corporate voice and data network. This document provides an overview of the solution architecture and describes the protocols used to ensure the confidentiality of voice and data communications.

Solution Architecture

The Teleworker Solution is one in a series of applications developed for the Mitel 6000 Managed Application Server and is designed to take advantage of that platform's simplicity, security and reliability. The specific purpose of the Teleworker Solution is to support remote connections to any network employing Mitel's proprietary MiNET signaling protocol for Voice –over –IP (VoIP). In practice, this means any network using the Mitel 3300 Integrated Communications Platform (ICP) and the Mitel SX-200® Integrated Communications Platform (ICP).

The Teleworker Solution consists of two elements. The first is an application (or "software blade") that is downloaded to the 6000 Managed Application Server from the Mitel Applications Management Center. Once installed and configured, the application allows the 6000 Managed Application Server to function as a proxy for remote phones requiring access to the corporate voice network. The solution offers several features that are designed both to improve voice quality over the Internet and to reduce bandwidth requirements between the corporate office and remote locations. The second element of the solution is the remote phone. This is a dual-port, dual mode Mitel 5215 or 5220 IP Phone (with or without Line Interface Module) that is configured to operate in Teleworker mode. The following diagram illustrates the two supported deployment options:



In the first, the Teleworker Solution gateway is configured to function as the corporate firewall and gateway. This is a typical scenario in a small business setting and allows the customer to take advantage of the built-in firewalling capabilities of the 6000 Managed Applications Server. (For more information on these capabilities, please refer to the document titled "Security and the Mitel Networks 6000 Managed Application Server.")

The second option is intended for situations where there is an existing corporate firewall. If this is the case, the Teleworker Solution gateway can be installed in the corporate DMZ. As illustrated on the previous page, the recommended configuration at the remote location is to plug the Internet connection into a standard cable/DSL router capable of providing Network Address Translation (NAT) and Dynamic Host Configuration Protocol (DHCP). The phone is then connected to the router and the teleworker's PC is connected to the second port on the back of the phone. Note that when the PC accesses the Internet via the phone, the phone does not interfere in any way with the data stream. The phone does, however, provide prioritization of the voice packets, ensuring better voice quality with minimal or no impact to the data connection. Installation of the Teleworker Solution is simple and is typically accomplished in less than 30 minutes.

The technician begins by loading the 6000 Managed Application Server software, which includes the Linux operating system, onto a standard Intel-compatible computer. Installation is fully automatic and requires no Linux knowledge. Finally, the installer accesses the server's web-based management interface (the "server manager"), enters the server account ID number (the server account ID is provided as part of the ordering process) and downloads the Teleworker Solution software blade.

To configure the blade, the technician clicks on "Teleworker Solution" in the server manager and enters the following settings:

- Teleworker Solution Status: set to "enabled"
- Mitel ICP Address: specifies the IP address of the ICP that will accept connections from remote IP sets
- Select the appropriate type of the ICP from the menu and enter the system ID.
- Enable G.729 transcoding: If the ICP provides support for G.729a transcoding, this option should be left at "no" (the default setting). Otherwise, it can be set to "yes" to reduce bandwidth requirements
- If there are multiple teleworkers at this site, enable local streaming to improve performance
- Configure any optional settings, which are described in the Teleworker Solution Blade Guide



White Paper

To configure the IP phone, the administrator powers up the phone, holds down the "7" key and, when prompted, enters the Internet-routable IP address of the Teleworker Solution gateway. This information is stored by the phone in NVRAM (Non-Volatile Random Access Memory).

At this point, the phone can be taken off-site and plugged into any broadband Internet connection via a cable/DSL router, as described above. When powered up, the phone will first obtain a local IP address from the cable/DSL router and then download its software from the Teleworker Solution gateway at the corporate office. When the download completes (generally in less than a minute), the phone again connects to the Teleworker Solution gateway and the server in turn connects to the Mitel ICP address that was entered on the blade web panel. Under normal circumstances, this entire process is automatic and requires no special configuration at the remote location, within 2 minutes, dial tone is achieved.

Voice Networking

To ensure the confidentiality of communications, all voice packets passed between the remote IP phone and the Teleworker Solution gateway are encrypted using the Secure Real-time Transport Protocol, a security profile for RTP.

RTP

The Real-time Transport Protocol (RTP) is an Internet protocol standard that specifies a way for programs to manage the real-time transmission of multimedia data such as voice or video. Originally specified in an Internet Engineering Task Force (IETF) Request for Comments (RFC1889) RTP is commonly used in Internet telephony applications. RTP does not in itself guarantee real-time delivery of multimedia data, since this is dependent on network characteristics. It does, however, provide tools to help manage the data as it arrives to best effect. (For example, an application can be configured to drop voice packets that are seriously delayed since audio dropouts tend to be less disruptive to human perception than echo or delay.)

Secure RTP

Secure RTP is a security profile for RTP that adds confidentiality, message authentication and replay protection to that protocol. Specifically, Secure RTP defines a set of default cryptographic transforms and allows new transforms to be introduced in the future.

The security benefits of Secure RTP include:

- Confidentiality of the RTP payloads, as well as protection against replayed packets
- Low bandwidth cost, i.e., a framework preserving RTP header compression efficiency, and limited packet expansion
- Low computational cost
- High tolerance to packet loss and re-ordering, and robustness to transmission bit errors in the encrypted payload

Secure RTP is ideal for protecting VoIP traffic because it can be used in conjunction with header compression and has no effect on IP Quality of Service (QoS). These attributes provide significant advantages, especially for voice traffic using low bit rate voice codecs such as G.729.

CAST-128

Secure RTP allows for the fast encryption of a voice stream using one of a number of encryption algorithms. The specific algorithm used by the Mitel Teleworker Solution to encrypt both the voice stream and MiNET signaling is the CAST-128 algorithm, documented in RFC2144.

Belonging to the class of encryption algorithms known as Feistel ciphers, CAST-128 is operationally similar to the Data Encryption Standard (DES) but uses a newer, larger key size. In a Feistel cipher, the input is broken into two blocks of equal size, generally called left and right, which are then repeatedly cycled through the algorithm. At each cycle, a hash function is applied to the right block and a randomly generated key. The result of the hash is XOR-ed into the left block (using the Boolean algebra function Exclusive-OR). The blocks are then swapped. The XOR-ed result becomes the new right block and the unaltered right block becomes the left block. The process is then repeated a number of times (rounds). Exclusive-OR encryption requires that both the encryptor and the decryptor have access to the encryption key, but the encryption algorithm, while extremely simple, is also extremely secure. The CAST-128 encryption algorithm is designed to use a key size that can vary from 40 bits to a maximum of 128 bits. The longer the encryption key, the more difficult it is to decrypt the file. (Every bit added to the length of the key doubles the number of tries that would be required to break the encryption through brute force.) The Teleworker Solution uses the most secure method of CAST-128 encryption with 16 rounds and a 128-bit key (also known as CAST5-128). Using a computer capable of one million calculations per second, it would take roughly 12 days to crack a 40-bit encrypted message by brute force but 10 to 25 years to crack a message encrypted with a 128-bit key.

MAC Address Restriction

In addition to protecting the confidentiality of the voice stream and the MiNET signaling, the Teleworker Solution is designed to prevent unauthorized remote phone users from gaining access to corporate voice resources. This is accomplished by restricting access to specified Mitel 5215 or 5220 IP Phones (Dual Mode), based on a unique identifier sent by the phone to the Teleworker Solution server in a MiNET control message. That unique identifier is the MAC (Media Access Control) address of the phone. The first time a 5215 or 5220 IP Phone attempts to send a registration message to the Teleworker Solution gateway, its MAC address is automatically logged and entered into a table that is displayed on the solution's web interface. By default, the phone is disabled and therefore will not be able to connect to the ICP. To allow access, the administrator must set the phone's entry to enabled by placing a check mark in the box next to the MAC address and clicking the "Update" button. It is also possible to enable specific phones by manually adding their MAC addresses to the table. Each phone's MAC address is printed on a label on the back of the set. If a large number of phones need to be installed, the administrator can enter an Installer Password in the configuration panel of the Teleworker Solution gateway. If such a password is set, the phone will prompt for it upon its

initial connection to the Teleworker Solution gateway. The installer then enters the password using the phone keypad and the Teleworker Solution gateway then enables that phone's MAC address for future connections.

For convenience, the table also allows a description to be entered for each phone. If the entry is added through the automatic registration process, the default description is the IP address of the phone.

Resources

Secure Real-time Transport Protocol

<http://www.ietf.org/internet-drafts/draft-ietf-avt-srtp-05.txt>

RFC 2144: The CAST-128 Encryption Algorithm

<http://www.ietf.org/rfc/rfc2144.txt>

Data Security

The Teleworker Solution offers several options for customers requiring a secure data connection between the remote site and the corporate office. If the customer has an existing Virtual Private Network (VPN) using IPSEC or any other encryption protocol, the Teleworker Solution can co-exist with that service. These VPN solutions may involve on-premise equipment (such as "VPN appliances") or use software installed on a desktop or laptop. In either scenario, the Teleworker Solution provides a secure voice connection while the existing equipment continues to secure the data connection. For customers that do not have an existing VPN solution, the Teleworker Solution supports two options:

1. The Teleworker Solution at the corporate office can be linked to a system at the remote office running the Mitel 6000 Managed Application Server software in a secure IPSEC VPN. This extends the corporate network into each of the remote offices and allows for the full access of network resources by systems in the remote offices. The Mitel IPSEC VPN offering includes the use of 3DES encryption and manages the exchange of IPSEC keys through the interaction of each Teleworker Solution and 6000 Managed Application Server with the Mitel Applications Management Center (AMC). The AMC acts as a trusted broker and provides a reliable mechanism for the secure exchange of IPSEC keys between servers.
2. For offices that wish only to enable access for specific remote desktop or laptop PCs, the Teleworker Solution includes full native support for the high-encryption version of the VPN software included with Microsoft Windows, version 98 and up (a free add-on is available for Windows 95). This software is based on the Point-to-Point Tunneling Protocol (PPTP) which was developed by a consortium of vendors led by Microsoft. Starting with release 2.0, the Teleworker Solution also supports the Layer 2 Tunneling Protocol with IP Security (L2TP/IPSec) as an alternative to PPTP. A client for L2TP/IPSec is included with Microsoft Windows 2000 and Windows XP, and is available as a free download for Windows 98/Me and NT 4.0.

Background on PPTP

In its earliest implementation, PPTP used an authentication protocol called MS-CHAP which was found to be insecure. Microsoft corrected the deficiencies and released a new authentication protocol called MS-CHAPV2. The MS-CHAPV2 protocol operates as an encrypted mutual authentication handshake. No passwords, in either clear text or encrypted form, are passed during authentication setup.

In addition to these measures, the Teleworker Solution requires both 128-bit and stateless encryption for PPTP. These address the known security issues inherent with the original PPTP protocol release, which included:

- Clear text/encrypted password exchange during authentication
- Clear text passwords on the server
- 40-bit encryption
- Encryption state carried between packets

In summary, the Teleworker Solution will not allow connections from PPTP clients that do not support all of:

- MS-CHAPV2
- Encrypted passwords on the server
- 128-bit encryption
- Stateless encryption

There have been no reported issues with the security of PPTP when configured in this fashion.

Background on L2TP/IPSec

L2TP/IPSec is a combination of Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP), using standard IPsec Encapsulated Security Payloads (ESP). Data packets are first encapsulated with a PPP header, then an L2TP routing header. This package is then wrapped with a UDP header and encrypted with IPsec before being sent across the Internet. Although it requires more overhead than PPTP, it is considered to be more secure.

Resources

Point-to-Point Tunneling Protocol FAQ

<http://www.microsoft.com/ntserver/ProductInfo/faqs/PPTPfaq.asp>

RFC 2637 - Point-to-Point Tunneling Protocol (PPTP)

<http://www.ietf.org/rfc/rfc2637.txt>

Security Architecture for the Internet Protocol (IPSEC)

<http://www.ietf.org/rfc/rfc2401.txt>

Microsoft L2TP/IPSec VPN Client FAQ

<http://www.microsoft.com/windows2000/techinfo/howitworks/communications/remotearchess/l2tpclientfaq.asp>



White Paper

www.mitel.com



North America

(613) 592 2122
1 800 648 3579

Benelux

Tel: +31 (0)30 85 00 030
Fax: +31 (0)30 85 00 031

Middle East

Tel: +971 4 3916721
Fax: +971 4 3915288

Latin America

(613) 592 2122
1 800 648 3579

Italy

Tel: +39 02 2130231
Fax: +39 02 21302333

South Africa

Tel: +27 82 559 8688
Fax: +27 11 784 6916

UK

Tel: +44 (0)1291 430000
Fax: +44 (0)1291 430400

Germany, Switzerland, Austria

Tel: +49 (0)211 5206480
Fax: +49 (0)211 52064899

Asia-Pacific

Tel: +852 2508 9780
Fax: +852 2508 9232

France

Tel: +33 (0)1 61 37 00 90
Fax: +33 (0)1 61 37 00 99

Portugal and Spain

Tel: +34 91 350 66 33
Fax: +34 91 350 70 14

THIS DOCUMENT IS PROVIDED TO YOU FOR INFORMATIONAL PURPOSES ONLY. The information furnished in this document, believed by Mitel to be accurate as of the date of its publication, is subject to change without notice. Mitel assumes no responsibility for any errors or omissions in this document and shall have no obligation to you as a result of having made this document available to you or based upon the information it contains.

M MITEL (design) is a registered trademark of Mitel Networks Corporation. All other products and services are the registered trademarks of their respective holders.

© Copyright 2005, Mitel Networks Corporation. All Rights Reserved.

GD 7525 PN 51005786RC-EN