

DESIGN GUIDE

DRACO SIRA - SECURE IP REMOTE ACCESS GATEWAY

When You need more than a network for secure remote workers



SMART STRATEGIES
FOR MANAGING
YOUR REMOTE WORKERS

TABLE OF CONTENTS

SMART STRATEGIES FOR WORK AT HOME COMPUTER SECURITY	03
TIP # 1 – Educate your workers with basic security knowledge	04
TIP # 2 – Set up a VPN access point for the work-at-home employee	05
TIP # 3 – Develop two level password protection.....	06
TIP # 4 – USB security	07
TIP # 5 – Personal Devices	08
TIP # 6 – Backup Plans	09
HOW IHSE CAN HELP WITH YOUR WORK-AT-HOME SYSTEM	10
THE TREND TOWARD IP CONNECTIVITY	10
THE NEED FOR AN ADVANCED KVM REMOTE IP ACCESS SOLUTION	12
MATRIX ATTACHED REMOTE IP CONFIGURATION	14
OPERATING FEATURES OF THE DRACO VARIO SECURE IP REMOTE ACCESS GATEWAY	14
USE CASE SCENARIOS	15
LOCAL CONNECTIVITY OVER LAN	15
LONG-DISTANCE CONNECTIVITY OVER WAN	15
HOW TO DESIGN A KVM SYSTEM: Main Office/Remote Office	16
IHSE KVM FUNCTIONAL DESCRIPTION	17
KEY FEATURES AND BENEFITS OF SIRA	18
IHSE SIRA NETWORK SOLUTIONS	19

SMART COMPUTER SECURITY STRATEGIES FOR REMOTE WORKERS

If you or your employees are working from home, you'll need this advice to secure your company data and assets.



Remote workers present a unique challenge to protecting confidential company data because remote work environments don't have the same safeguards in place that would be found in an office environment. When workers are at the office, they are typically behind several layers of security control and firewalls. While there may be different levels of security in an office environment it becomes a much higher risk to the company to prevent security breaches once a computer leaves the office security perimeter.

There is no specific size of company that is immune to cyberattack. Adding to this issue, remote work has become a necessity for many organizations which makes it more important to have security policies in place. Today, organizations around the world are sending hundreds of thousands of workers home in response to the work-at-home requirements for the COVID-19 outbreak.

In normal situations, the risk of security is between the servers and end user computers. Working outside the confines of the company office network now adds external concerns when workers access company data from a public internet or consumer-grade home office network. Working outside the office adds additional concerns of system access, bandwidth requirements and data sharing

across multiple network points. Now it becomes much more important than just changing your email password periodically. While companies are adjusting to the increase from the work-from-home employee, companies must now keep cybersecurity in mind to protect devices and data just as they would in the office.

In light of the COVID-19 crisis, many companies are rushing to create a work-at-home plan. Although many of these companies did not have much time to prepare, practicing safe online methods will only further support the way your business continues to function and operate securely. Online hackers and cyber criminals are ready to gain access to your computers, laptops and Wi-Fi devices because they know your security measures may not be as robust as they typically are at the office.

To assist with helping our customers with the most critical concerns of a work-at-home plan, we've compiled a range of best-practice tips and working strategies to minimize this potential risk - whatever your business vertical or business size.

Although not a complete list of critical strategies, these 6 tips compiled from some of the best resources on the web will assist you develop guideline policies to develop your work-at-home strategies.

TIP # 1 EDUCATE YOUR WORKERS WITH BASIC SECURITY KNOWLEDGE



The bottom line is simple: nobody in your organization will care about data security, IP protection or privacy policies until you show them why it's important, how it impacts their roles and what they can do to prevent cyberattacks. A comprehensive cybersecurity awareness training plan should be developed to educate employees on common threats they are likely to face in their daily jobs.

People working from home must be provided with basic security advice: to beware of phishing emails, to avoid use of public Wi-Fi, to ensure home Wi-Fi routers are sufficiently secured and to verify the security of the devices that they use to get work done. It is likely that attempts to subvert security using phishing attacks will increase at this time.

Employees should be particularly reminded to avoid clicking links in emails from people they do not know, and installation of third-party apps should be confined to bona fide app stores, even on personal devices.

Here are some basic threat issues every worker should understand.

- **Phishing:** Employees should be educated on how to spot and report phishing and the dangers of interacting with suspicious links or entering credentials on a spoofed page.
- **Physical security:** Physical security requirements can vary on an organization's nature. Since businesses should already have a physical security policy in place, this is a great opportunity to make sure employees understand the parts of the policy that apply to them, such as locking desk drawers and rules about allowing guests into the home office.
- **Desktop security:** Outline the potential consequences of failing to lock or shut off computers at appropriate times and plugging unauthorized devices into workstations.
- **Wireless networks:** Explain the nature of wireless networks and outline the risks of connecting to unfamiliar ones.
- **Password security:** Complex password requirements and prompting employees to change their passwords on a regular basis should already be enforced, but password security training is still important to explain the risks involved in reusing passwords, using easy-to-guess passwords, and failing to change default passwords immediately. Authorized password management tools may also be covered
- **Malware:** A training session on malware should define the types of malware and explain what they are capable of. Users can learn how to spot malware and what to do if they suspect their device has been infected

TIP # 2

SET UP A VPN ACCESS POINT FOR THE WORK-AT-HOME EMPLOYEE



If your employee is a new work at home user it is important to provide them with a secure, reliable way to connect to the company's network systems. One way to do this is to use a remote-access virtual private network (VPN). VPN services provide an additional layer of security, which provides a way to hide the user's IP address while encrypting data transfers and masking the user's location. Here is what you need to know about VPN's if you are considering taking advantage of the technology.

- **Secure Connections:** Companies use remote-access VPNs to establish secure connections between their networks and the devices used by offsite employees. Once connected, the employees are able to access the resources on the network, just as if their devices were physically plugged into it.
- **Encrypting Data:** A remote-access VPN works by creating a virtual tunnel between an offsite employee's device and the company's network. This tunnel goes through the Internet or another type of public network. The tunnel and the data traveling through it are protected by encryption and security protocols, which keeps the data private and secure.

- **Data Security:** Using a remote-access VPN offers several advantages for businesses. The most important benefit is data security. When offsite employees send data through a VPN, it is encrypted, so if hackers happen to capture the data, they won't be able to use it.

Larger organizations already have a VPN service in place and should check they have sufficient seats to provide this protection across their employee base. Smaller enterprises may need to appoint a VPN provider.

Lastly, for some use cases, you can also set up encrypted remote connections into a remote desktop or other individual server. Many of these connection types (RDP, HTTPS, SSH, Virtual Machines) include encryption as part of their service direction and do not require an additional VPN or other encryption service to secure the data in-transit.

TIP # 3

DEVELOP TWO LEVEL PASSWAORD PROTECTION



Just about any account you own on the internet is prone to being hacked. After numerous widespread breaches through the past few years, tech companies have been working together to develop a standard that would make passwords a thing of the past, replacing them with more secure methods like biometric or PIN-based logins that do not require transferring data over the internet.

But while those standards are still being adopted, the next best way to secure your accounts is two-factor authentication, or 2FA. This is a process that gives web services secondary access to the account owner in order to verify a login attempt. Typically, this involves a phone number and / or email address. This is how it works: when you log in to a service, you use your mobile phone to verify your identity by either clicking on a texted / emailed link or typing in a number sent by an authenticator app.

- **Secure Connections:** Run a password audit: Your Company needs to audit employee passcodes. That doesn't mean requesting people's personal details, but does mean passcodes used to access any enterprise services are reset and redefined in line with stringent security policy. Alphanumeric codes, use of two-factor authentication should become mandatory, and you should ask your people to apply the toughest possible protection across all their devices. You should also ensure all your business-critical passwords are securely stored in the event anything happens to key personnel.
- **Set up two-factor authentication:** Having a strong password often isn't enough, for example, if your credentials are leaked in a data breach. Two -factor authentication (2FA) and two-step verification (2SV) involve an additional step to add an extra layer of protection to your accounts. The extra step could be an email or text message confirmation, a biometric method such as facial recognition or a fingerprint scan, or something physical, such as a USB fob.

TIP # 4 USB SECURITY



USB Portable and mobile storage devices are significant players in most corporate offices and are commonly used in home offices as well. However, for such a small device the USB flash drive can cause big security headaches. Even if you have a robust end-point security policy, workers without knowledge of how crucial it is to follow USB security guidelines will use these devices to copy both non-critical and potential confidential information for home use. Ensuring proper protection with a best practices policy and strict enforcement offers significant risk reduction—and can prevent long nights on data breach investigations.

Typical computer security breaches are more traceable but a flash drive is more difficult to monitor, especially after the employee leaves the work office. The best policy for workers is *never use a thumb drive if you don't know where it came from* and do not continue to use one if you have plugged it into a system for whose safety you cannot honestly vouch.

If you must use USB flash drives, it is important to follow these simple guidelines for USB security practices.

- **Enable USB functionality on a need-to-have basis.** Disable storage devices on computers with access to sensitive information. It will limit exposure and reduce the risk of unauthorized data being transferred away from your organization.
- **Enforce USB scanning on all corporate computers whenever a thumb drive is plugged in.** This can help ensure no malware or malicious programs are on the drive. Allow only corporate signed and approved applications to be run from the drive.
- **If possible, issue USB devices with unique serial numbers** tagged in the firmware, as well as etched on the outside cover.
- **Blocking Physical USB ports on company owned computers used for remote workers** – the most radical approach is to cover the USB ports with tamper-proof tape.

TIP # 5 PERSONAL DEVICES



Many businesses issue remote workers with a dedicated laptop, which can be centrally managed and configured in accordance with internal data policies, as well as protected by the company's choice of endpoint protection. However, if remote workers are using their own PC equipment from home, it is vital to ensure that they have installed reputable anti-virus tools and follow corporate guidelines for network configurations, firewall protections and password security.

If you work at an organization with an efficient IT team, they may be installing regular updates, running antivirus scans, blocking malicious sites, etc., and these activities may be transparent to the workers.

There is a good chance that workers have not followed the same protocols with their personal computer as are mandatory at work. Furthermore, the company can likely afford higher end technical controls than workers can personally. Without those running in the background, a personal computer is not safe for work information because it could be compromised by a third party. Essentially, by introducing a personal computer to a work network, even remotely, it puts the company network at risk, and potentially the worker at risk, accepting the potential liability of extensive corporate damages through violations of policy, practices or both.

- **Using personal devices and networks:** Many workers will be forced to use personal devices and home networks for work tasks. These will often lack the tools built in to business networks such as strong antivirus software, customized firewalls, and automatic online backup tools. This increases the risk of malware finding its way onto devices and both personal and work-related information being leaked.

- **Lock your device** If you do have to work in a public space, or if you live with people who you can't share work information with, then it's important to keep your device secure. Password-locking your device will usually encrypt its contents until someone enters the password.

- **Don't Use Work Devices for Personal Needs:** Easier said than done, we know, especially when the mirror image of this rule (BYOD, or Bring Your Own Device) is so prevalent. Still, just as it's important to carve out boundaries between work life and home life while working from home, the same is true of those devices you use in these settings.

"Make sure that you have a malware protection software installed to monitor activity and keep out unwanted intruders. Also, make sure both your personal and business data are hosted on a secure platform that encrypts the files. Ideally, look for a platform that has built-in security timeouts if a device is left inactive too long and allows you to wipe data remotely in the event that your device is lost or compromised."
– Brian Schrader, Co-Founder and President of BIA

- **Lock Your Doors.** If you bring your work computer home or tend to work remotely, confidential corporate information could be at risk. When you get in the habit of always locking your doors, you have taken a key step toward improving your home office's security. Don't subject yourself to the stress of a stolen work computer or harm your company by letting its data out into the wild.

- **Formalizing Working from Home and Remote Work Policies.** While good technologies and policies help, the truth is that the very employees who make the business successful are a primary avenue of risk. General work from home and remote work policies on computer and internet use can help, and these policies can be enforced with both technical and administrative controls.

HOW IHSE CAN HELP WITH YOUR WORK-AT-HOME SYSTEM



Figure 1: IHSE SIRA models of secure gateway and remote user access modules

At IHSE we are always looking for ways to improve the performance of our products to best serve your needs for quality video image and transparent mouse and keyboard interactions. Our latest models of KVM extenders now bring you the next level of performance by allowing operators to seamlessly interact between our baseband KVM extenders and switch products through a secure network interface.

THE TREND TOWARD IP CONNECTIVITY

Organizations around the globe are taking advantage of IP technology to run their businesses and to communicate between staff, with customers and external agencies. They recognize the benefits and are rapidly embracing them, to gain efficiency, lower costs and add greater flexibility in their day-to-day operations.

IP technology enables new opportunities in the way businesses can operate and work together. People can connect simply and easily to remote computers to access applications that allow them to inter-communicate, manage complex data and control distant operations.

Traditional IP network-based tools have been available for several years and operate effectively. These allow operators using locally-installed client software to control compatible remote servers. However, client-server solutions have limitations that affect their usability. These limitations are predominantly in dynamic performance and security; both of which are serious considerations in most professional applications. The majority of client-server solutions require additional hardware and the installation and setup of complex software.

IHSE's new Secure IP Remote Access Gateway (SIRA) overcomes the problems associated with security, accessibility, immediacy and image quality of traditional packetized remote IP-connection to distant computers using client-server models. SIRA's premise is simple and straightforward. It provides KVM extension over an IP network by extending keyboard, mouse, USB and video signals; in the same manner that IHSE's traditional KVM extenders transfer signals. It means that a remote operator can access any desired computer, at any distance away, using a keyboard and mouse as though they were physically located alongside that computer.



Figure 2: Example of connections between remote locations and local connections

The signals passed between the operator and computer retain full integrity, have the highest possible transmission rate and can be switched on demand. Most importantly, total system security is maintained. The only data transferred over the network is visual images and USB commands. So it is impossible to mount cyber-attacks that take operational control of computers or plant malicious software.

Backup for evacuation scenarios

The SIRA IP Gateway not only enables workers to continue working in the most secure and effective way whilst isolated at home but permits secondary back up

facilities to be created for use should the primary center be compromised in any way. In the current situation this may be when an operator falls ill and the whole control area needs to be evacuated and cleaned before it may be used again.

SIRA can be incorporated into an existing IHSE KVM system or included as part of a remote operating facility as a point-to-point extender; allowing essential workers to access crucial systems with total security, wherever they happen to be. And ensure that their organization remains operational now and viable in the future.

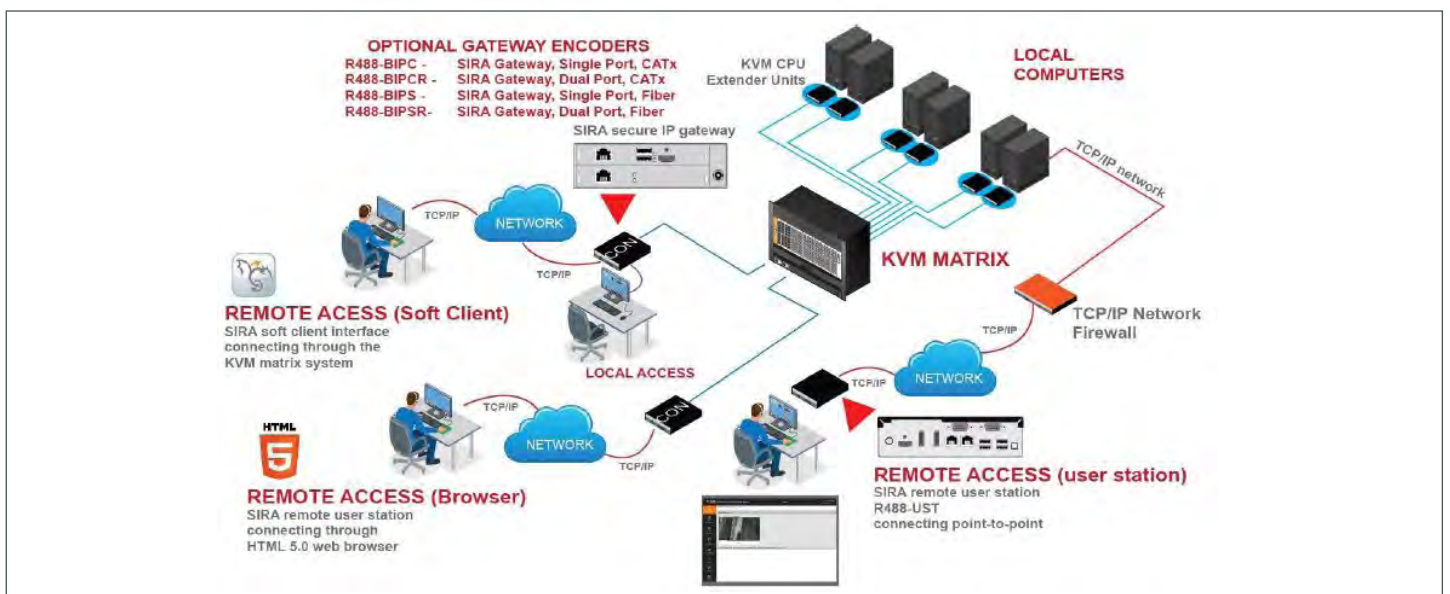


Figure 3: Flow diagram of connections for SIRA IHSE Secure IP Remote Access Gateway (SIRA) connecting the remote worker securely and safely

THE NEED FOR AN ADVANCED KVM REMOTE IP ACCESS SOLUTION

Users require a system that is simple to install and set up, flexible in operation, compatible with all existing equipment, offers best possible performance and maximum security. One that provides direct access to a remote computer without the delays and inconsistent performance experienced in most client-server setups. The Draco vario Secure IP Remote Access Gateway (SIRA) provides a solution to this critical operational requirement. It operates within two spheres of application:

■ Standalone remote IP connectivity

Acting as a simple KVM extender solution between a single computer, or several computers, and a remote user, using only keyboard video and mouse data transmission over an IP network. A user may connect directly to a single remote computer or manage multiple simultaneous sessions using a simple notebook or desktop PC and the supplied client software.

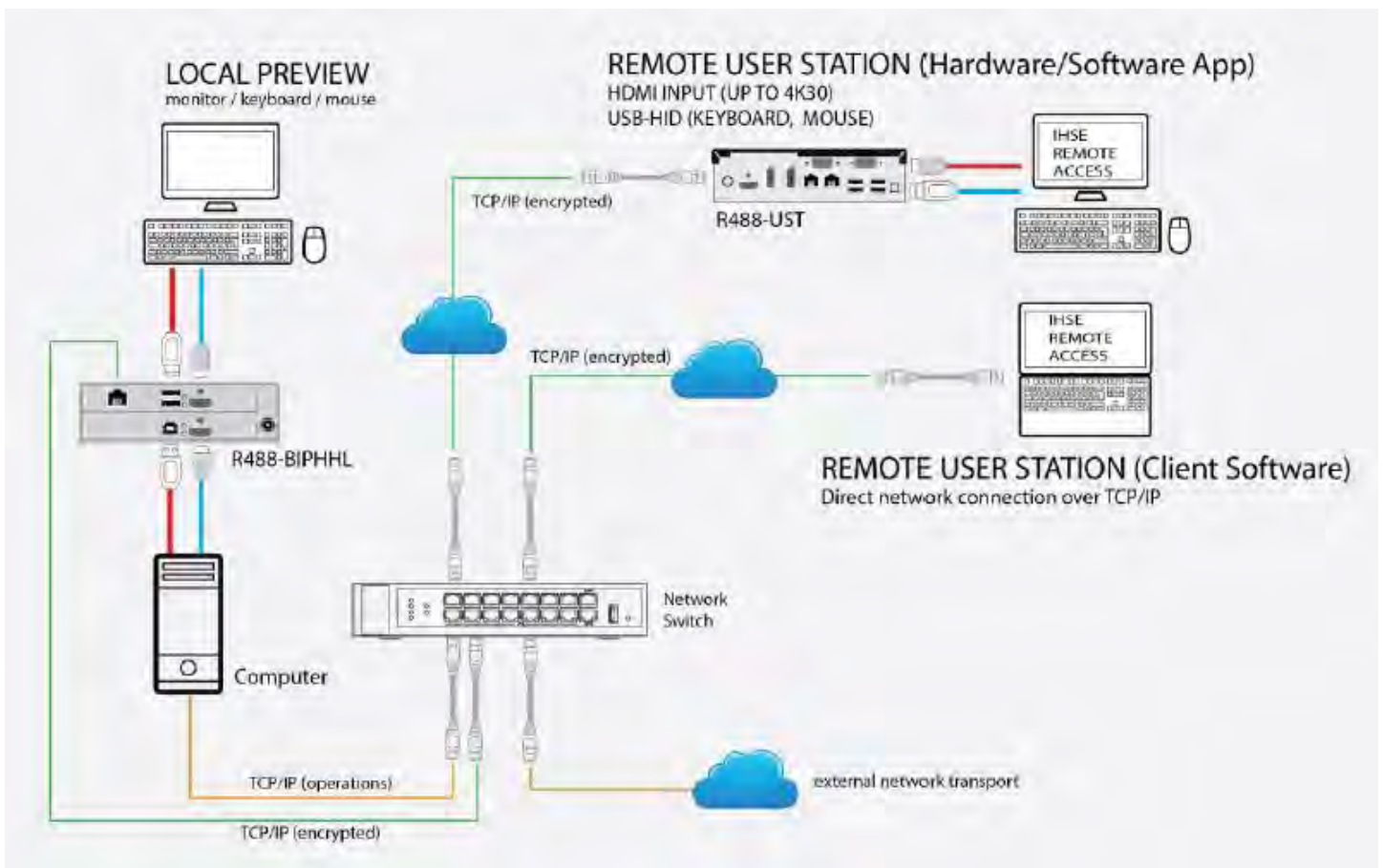


Figure 4: Schematic of connections for remote users stand alone

■ KVM matrix-connected connectivity

As an extension to a larger Draco tera KVM system to provide remote access to the switch by a remote user over an IP network. This configuration gives the user full

connection to all source computer devices connected to the Draco tera switch.

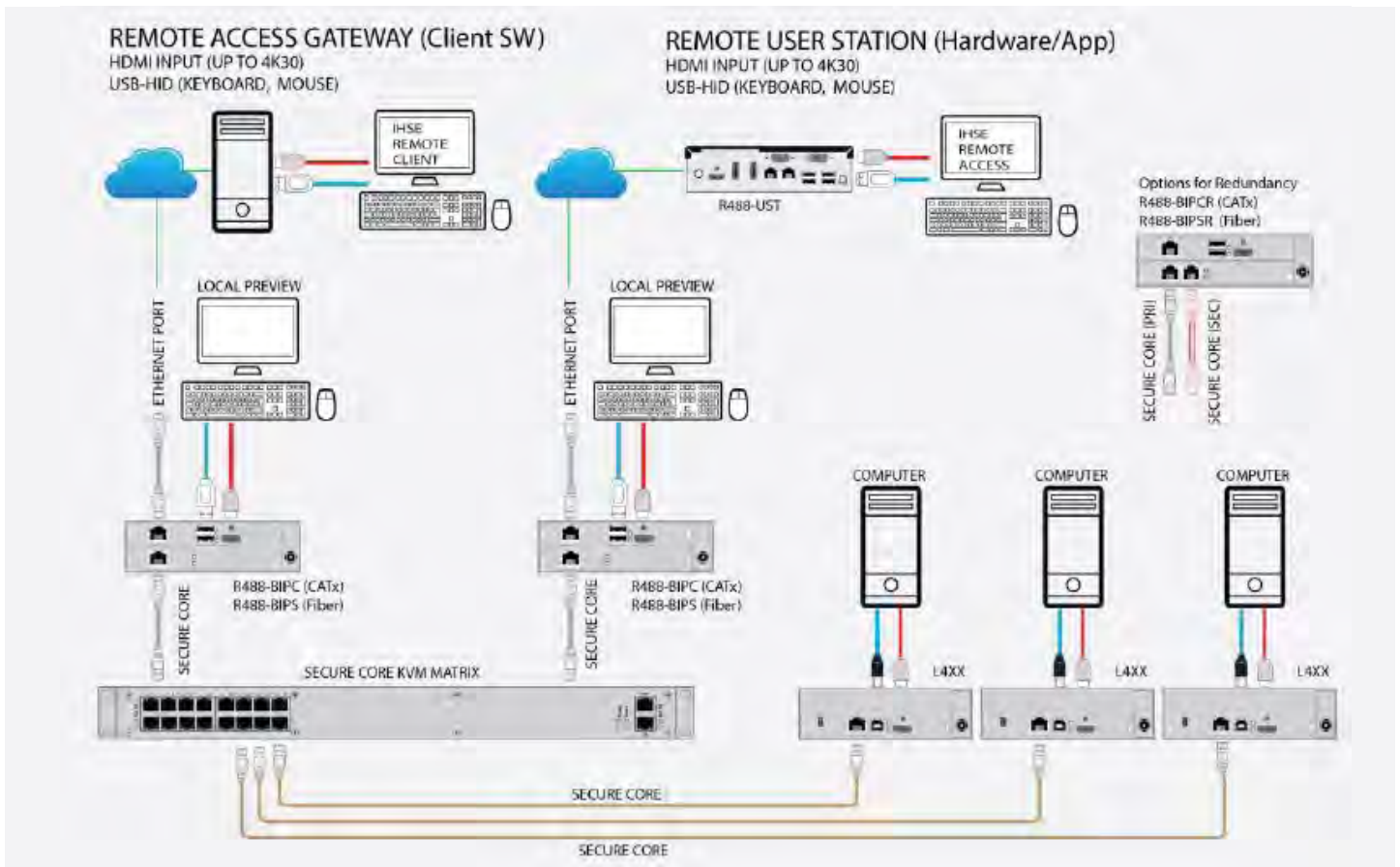


Figure 5: Schematic of connections for remoter users for multiple source connection

Standalone remote IP configuration

SIRA can operate in two modes: single-session and multi-session.

In single-session mode a computer with royalty-free soft client or HTML5.0 Browser acts as the decoder connected over an IP network to the SIRA encoder located locally to a single remote computer. Alternatively, a SIRA decoder K488-UST may be used with a standard video monitor, keyboard and mouse, without requiring an additional computer and soft client.

In multi-session mode, the SIRA decoder K488-UST provides remote access to multiple individual computers in mosaic layout over an IP network. The SIRA decoder can display several sources on a single display using quad-split or picture-in-picture image layouts. Images can be spread and duplicated over multiple user monitors. Inter-connection and transmission of information is essentially at computer video, USB and audio levels using the signals output from, and input to, the computer peripheral ports.

Unlike traditional client-server configurations there is no requirement for additional software on the client or server devices. All signal translation and transmission are undertaken within the SIRA encoder and decoder devices.

In operation, the user console, comprising video screen, keyboard and mouse, acts as though it is directly connected to the appropriate computer user interface ports. An operator has direct control over the computer using their own keyboard and mouse.

The standalone solution supports virtual media (VM) transport which allows USB devices including portable memory sticks, CD-ROM, NAS and other storage devices, to be attached at both server and user ends of the transmission link. Files can be transferred in both directions. For security and control, the system administrator sets and manages user rights to this feature.

MATRIX ATTACHED REMOTE IP CONFIGURATION

SIRA provides a convenient and highly effective method of remotely connecting to an existing KVM switching infrastructure. The objective of this configuration is to enable a remote user to interact with all computers on a direct connect KVM infrastructure as though they were physically located close to it. The user can be given the same access rights and accessibility to all computers on the network as an associate connected directly to the KVM switch. As with the standalone solution, there is no requirement for additional software on the client or server devices to be installed. All signal translation and transmission processes are undertaken within the SIRA encoder and decoder devices or client software which operates like a portable app with no software installation.

In operation, the user console of video screen, keyboard and mouse device acts as though they were directly connected to the appropriate computer user interface ports. Individual users are not limited to single remote KVM installations and can have access to multiple KVM switches in different locations provided with a local SIRA encoder.

remote client. It is processed and therefore manipulated and send across the network fully encrypted using RSA 2048 keys and selectable AES 128/256 encryption.

- Video data bits are delivered as a compressed stream through either continuous capturing of individual screen shots or the changes between frames (interframe compression) in order to save bandwidth.
- USB data is translated at either end of the transmission link for transfer in both directions between the SIRA encoder and decoder units to complete the connection to USB computer ports and USB-HID devices.

USER ACCESS AND RIGHTS

The user can securely access the remote computer down to the BIOS level of the source PC without any special software or drivers required. An active link to the source PC through the SIRA encoder and decoder is only established by request from the user. If no connection is established, KVM data is not transmitted onto the network.

Operators using SIRA to access remote computers can be

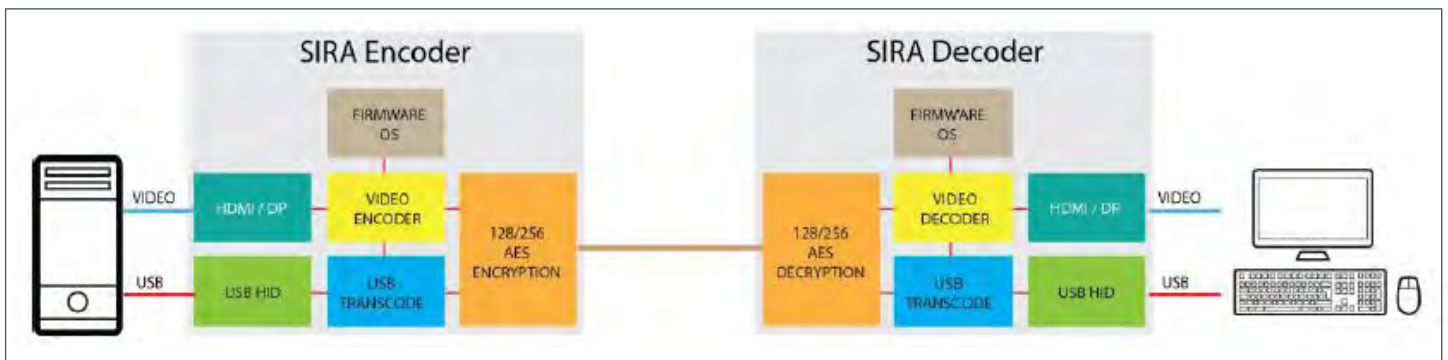


Figure 6: Signal connection diagram between encoder and decoder

OPERATING FEATURES OF THE DRACO VARIO SECURE IP REMOTE ACCESS GATEWAY

VIDEO AND USB TRANSMISSION

The video signals received from the remote computer are received and processed by a proprietary CODEC in the SIRA encoder that efficiently manages the compression and transmission of images via IP networks.

The video signal transmission process operates as follows:

- The Draco Secure IP Remote Access Gateway encoder provides only fixed EDID information to the graphics card of the host systems. There is no return channel for data transmission from the graphics card to the encoder and further on to the remote user.
- Capture of the video of the host PC output on the computer graphic card video port is not transferred as raw data to the

restricted in their operational functionality (e.g. video only access, blocking of certain defined keyboard characters etc.). This is based on user profiles outlining access options.

SECURITY CONSIDERATIONS

The SIRA system permits standard keyboard mouse and video signal transfer and USB mass storage-transfer of data under strict access controls. These guard against cyber-attacks by preventing hacker access to the host systems.

Accessing or manipulating the operating system of the Draco Secure IP Remote Access Gateway using these interfaces is impossible as the encoder only processes keyboard and mouse signals. The configuration of the SIRA operation systems is separated from the user interface and cannot be accessed.

In addition, the operating system of SIRA is firmware based. Changing the OS requires a reboot of the SIRA unit. The OS of SIRA is protected with an encrypted signature, once to protect the intellectual property of the encoder and a second time to avoid any kind of manipulation by third parties.

USE CASE SCENARIOS

LOCAL CONNECTIVITY OVER LAN

Typical application in-building, on-site or on-campus connection to single or matrix-connected computers to provide convenient access, physically separate operators or create back-up or emergency configurations.

LONG-DISTANCE CONNECTIVITY OVER WAN

Wide area network connection between remote locations for example to enable home working or disaster recovery.

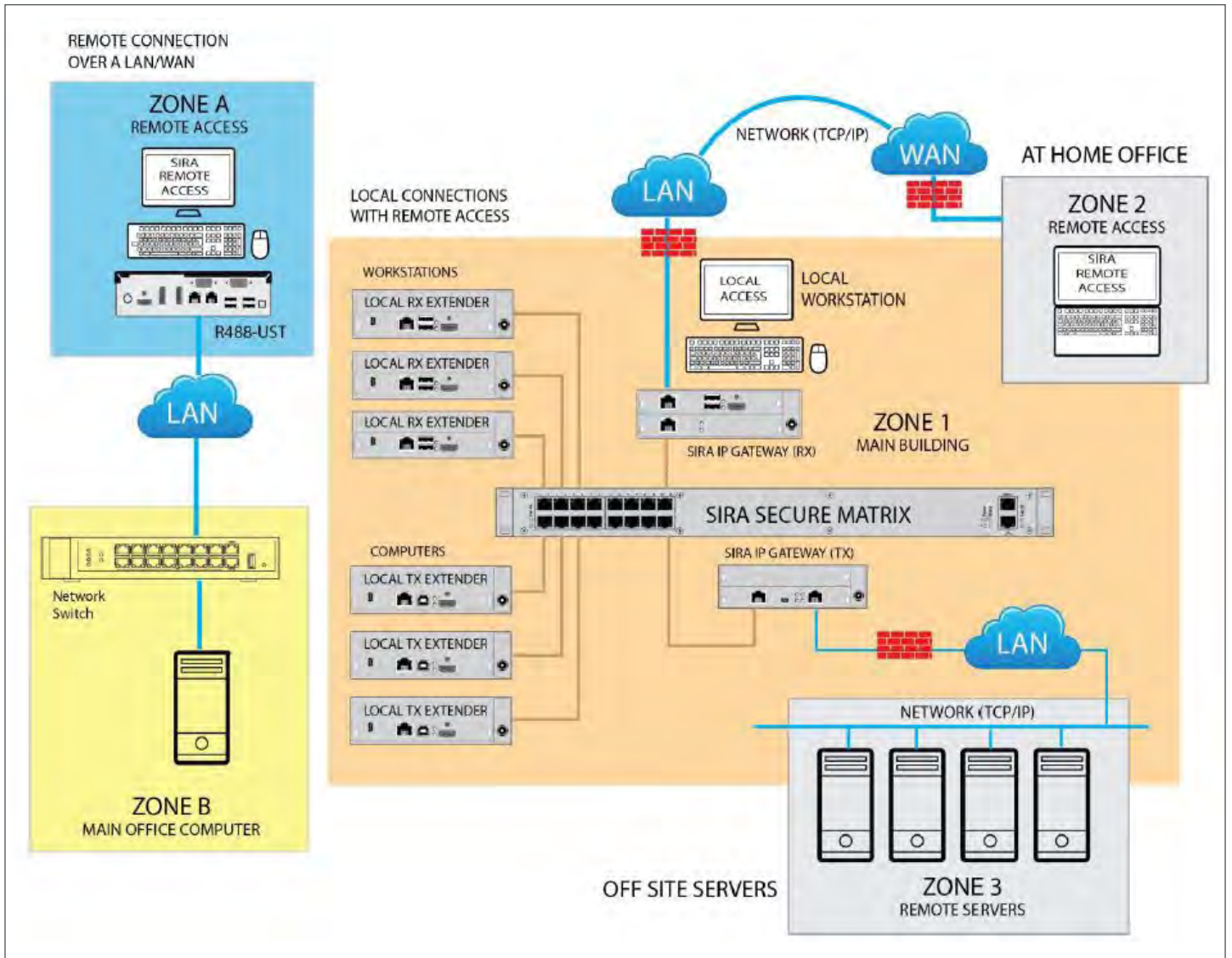


Figure 7: Overview of connectivity for KVM SIRA Systems

HOW TO DESIGN A KVM SYSTEM: MAIN OFFICE / REMOTE OFFICE

Factors to consider when designing a secure IP KVM system for work-at-home environments.

It is important to carefully consider the most appropriate KVM components for you for your specific application and requirements. In order to help find the best solution, you should start with some basics to create a materials list of need. Here are some important questions to consider:

■ Existing Computer Sharing Settings

- Determine the number of computers or servers you want to share now and what you expect may be needed in the future.
- What kind of peripheral devices (keyboard, mouse, trackballs, audio, etc.) will be connected to the computers?
- Determine the number of users who will need access externally and internally.
- How many users will need access from both external and internal workstations?
- How many users will need to have access to multiple computers simultaneously?

■ Required Video Format

- What video interfaces need to be connected. (DVI, HDMI, DisplayPort, VGA)
- What video resolutions need to be supported?

■ Connection types and distances

- Will you be using a Virtual Private Network (VPN) over a LAN or WAN?
- What are the distances between devices in the corporate office?
- Will you need Category 5e/6/7 or fiber interconnections?

■ Security and data protection

- What type of password protection and encryption will be used for work-at-home connections?
- Will LDAP or active directory be used to manage user log in?
- What type of backup or redundancy system will be incorporated?

If you need assistance to decide what KVM system would work best for your configuration, contact our technical design team at info@ihseusa.com. We can assist with recommendations, suggestions or special features you should consider when purchasing a KVM for work-at-home needs.

IHSE USA LLC

1 Corporate Drive
Cranbury, NJ 08512
USA

Tel.: +1 (732) 738 878 0
info@ihseusa.com
www.ihseusa.com

IHSE KVM FUNCTIONAL DESCRIPTION

Now that you know what to build the next part is to figure out what type of components will be needed to setup your KVM system.

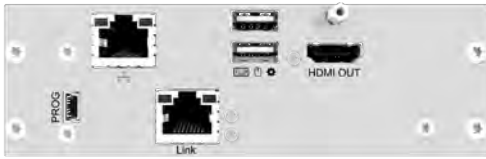
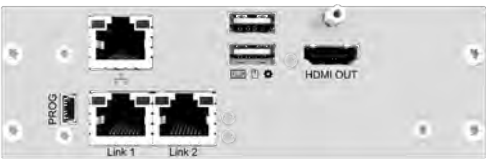




A SIRA KVM (KEYBOARD, VIDEO, MOUSE) MATRIX SYSTEM IS COMPOSED OF THESE BASIC PARTS:

Type of Device	Definition
<ul style="list-style-type: none"> ■ Extender, Transmitter (CPU) ■ for local connections ■ Point to point or matrix switch ■ Available in Fiber or CAT X 	<p>Signal transmitting extender device (CPU) connecting the source devices such as a Server, computer or video camera connections. From the CPU device a single RJ-45 (copper) is used to extend the transmitted data signal from the source to the matrix switch inputs or directly to a receiver device (CON). Typical signal devices connected include HDMI, DVI, VGA, USB, Audio and RS-232.</p>
<ul style="list-style-type: none"> ■ Extender, Receiver (CON) ■ For local connections ■ Point to point or matrix switch ■ Available in Fiber or CAT X 	<p>Signal receiving extender device (CON) accepting a single RJ-45 (copper) to accept a data path from the CPU or matrix switch. From the CON device, displays, interface devices or recording devices are connected to produce graphic images, USB connections, audio interconnects and serial data communications.</p>
<ul style="list-style-type: none"> ■ KVM Matrix Switch ■ Available in Fiber or CAT X 	<p>Matrix Switch (MS) allows CPU and CON devices to be connected into a centralized distribution method for sharing, switching and managing a large number of devices from a single point. The matrix switch can be controlled by keyboard Hot-Keys, a Java Tool Applet, or through a third-party control system via an API.</p>
<ul style="list-style-type: none"> ■ Secure IP Gateway 	<p>Signal encoder and decoder devices connecting a remote user to a physical KVM system through either a LAN or WAN connection.</p>

KEY FEATURES AND BENEFITS OF SIRA

SIRA PROVIDES A RANGE OF BENEFITS TO USERS:	
<p>Direct connection to standalone computers</p> <p>Directly connect remote computers in lights-out environments with centralized remote management of distributed computers.</p>	<p>Remote KVM matrix connection</p> <p>Remote connection to Draco tera KVM matrix systems over local and wide area TCP/IP networks. Ideal for fallback scenarios and standby operations.</p>
<p>Control distant computers to BIOS level</p> <p>Connection via external video and USB ports. No software or drivers to be installed on hosts.</p>	<p>High performance</p> <p>Native 4K30 video capability and embedded 16-bit audio. Connection to 4K60 Draco tera networks with built-in frame rate conversion.</p>
<p>Ease of installation</p> <p>No software or driver installation required. Uses Windows and Java-based client for Linux, Macs. HTML5.0 browser option.</p>	<p>Low IP complexity</p> <p>Limited data bandwidth requirement. No multicast. No IGMP settings nor any jumbo frame configurations. SIRA is designed for long-haul connections (WAN) as well as LAN and CAN scenarios.</p>
<p>Secure</p> <p>Incorporates 2-layer log-in authentication: SIRA access and Draco tera. IP masking to IP range and individual IP address levels. RSA2048 key, AES256-bit encryption. Administrator access control.</p>	<p>Maximum resistance to cyber-attack</p> <p>System operates using keyboard and mouse commands with no access to PC file system or OS through IP network.</p>
<p>Reliability and redundancy options</p> <p>Redundant power supply and link port configuration options.</p>	<p>Out of band operation</p> <p>Direct matrix control through keystrokes and OSD. Fallback and failsafe operation.</p>

IHSE SIRA NETWORK SOLUTIONS

PART NUMBERS		
 <p>A network module with a single RJ-45 port labeled 'Link', two USB ports, and an HDMI OUT port.</p>	R488-BIPC	<p>Secure IP Gateway, CON Module, Cat-X, for resolutions up to 3840X2160@30Hz, local KVM out, 2X USB, HDMI, RJ-45 for 1G LAN, RJ-45 for up to 140m KVM link over IHSE Secure Core Link.</p>
 <p>A network module with two RJ-45 ports labeled 'Link 1' and 'Link 2', two USB ports, and an HDMI OUT port.</p>	R488-BIPCR	<p>Secure IP Gateway, CON Module, Cat-X, for resolutions up to 3840X2160@30Hz, local KVM out, 2X USB, HDMI, RJ-45 for 1G LAN, RJ-45 for up to 140m KVM link over IHSE Secure Core Link. Redundant Secure Core Ports for closed loop connections</p>
 <p>A network module with a single RJ-45 port, two USB ports, and an HDMI OUT port.</p>	R488-BIPS	<p>Secure IP Gateway, CON Module, Fiber, for resolutions up to 3840X2160@30Hz, local KVM out, 2X USB, HDMI, RJ-45 for 1G LAN, LC Duplex for up to 10km KVM link over IHSE Secure Core Link.</p>
 <p>A network module with two RJ-45 ports, two USB ports, and an HDMI OUT port.</p>	R488-BIPSR	<p>Secure IP Gateway, CON Module, Cat-X, for resolutions up to 3840X2160@30Hz, local KVM out, 2X USB, HDMI, RJ-45 for 1G LAN, RJ-45 for up to 140m KVM link over IHSE Secure Core Link. Redundant Secure Core Ports for closed loop connections. Redundant Secure Core Ports for closed loop connections</p>
 <p>A network module with a single RJ-45 port, two USB ports, an HDMI OUT port, a USB port, and an HDMI IN port.</p>	R488-BIPHHL	<p>Secure IP Gateway, point to point connections, for resolutions up to 3840X2160@30Hz, local KVM out, 2X USB, HDMI, RJ-45 for 1G LAN. Matrix compatible with added components.</p>
 <p>A user station with a front panel featuring a power button, volume knob, and various ports: DC-IN, HDMI, DP, DP, COM 1, COM 2, 3.1+ audio, SS audio, and USB.</p>	K488-UST	<p>KVM EXTENDER, IP, Remote Access User Station, Video up to 4K30, USB-HID, Audio, RS232</p>

HOW HIGH-PERFORMANCE KEYBOARD VIDEO MOUSE
EXTENDER AND SWITCHING TECHNOLOGY ENABLES IMPROVED
PRODUCTION WORKFLOWS AND PRISTINE VIDEO DISPLAY



IHSE GmbH

Headquarters
Benzstr. 1
88094 Oberteuringen
Germany

Tel.: +49 (7546) 9248-0
info@ihse.de
www.ihse.de | www.ihse.com

IHSE USA LLC

1 Corporate Drive
Cranbury, NJ 08512
USA

Tel.: +1 (732) 738 878 0
info@ihseusa.com
www.ihseusa.com

IHSE GmbH Asia Pacific Pte Ltd

158 Kallang Way, #07-13A
Singapore 349245

Tel.: +65 (6841) 470 7
info-apac@ihse.com
www.ihse.com | www.ihse.com.cn

IHSE China Co., Ltd.

Room 814, Building 3, Kezhu Road
No. 233 Huangpu District
Guangzhou PRC

Tel.: +86 (189) 888 381 11
info@ihse.com.cn
www.ihse.com.cn

