

常问问题 • 2 月/2008 年

西门子工业安全 SCALANCE S 用 户指导手册

SCALANCE S, DHCP, Syslog, 防火墙, 虚拟专用网络, 网络地址解析/网络地址端口解析, 路由

http://support.automation.siemens.com/CN/view/109095166

目录

第一章 SCALANCE S 简介
第二章 DHCP 服务器4
2.1 DHCP 概述4
2.2 DHCP 组态4
第三章 Syslog9
3.1 Syslog 概述9
3.2 Syslog 组态9
第四章 防火墙11
4.1 防火墙概述11
4.2 防火墙组态11
第五章 虚拟专用网络
5.1 VPN 概述15
5.2 VPN 组态18
第六章 路由
6.1 路由概述
6.2 路由组态
第七章 NAT/NAPT
7.1 NAT/NAPT 概述31
7.2 NAT/NPAT 组态

第一章 SCALANCE S 简介

通过不同的安全措施的组合,例如防火墙,NAT/NAPT,路由以及VPN等,SCALANCE S612/613实现对自动化网络Cell的保护。这样对于自动化网络的数据侦探、随意操作、非法访问 是不可能的。

SCALANCE S612/613满足自动化工程应用环境的特殊要求,特别用于保证可用性和无故障操 作的场合,保护工厂和产品生产。与Softnet Security Client客户端软件一起,可以实现可伸缩性 的保护性能。通过使用Security Configuration Tool工具可以简单的使用SCALANCE S,并且组态安 全策略的方法简单,不需要专业IT安全知识。

SCALANCE S提供了以下的安全功能:

防火墙。支持状态包检测功能(Stateful Packet Inspection),可以过滤非IP报以及带宽限制。 所有内部网络设备被SCALANCE S保护。

安全的IPSec通讯。SCALANCE S可以通过组态配置成组。IPSec隧道在组内的SCALANCE S之间 建立,通过隧道,内部网络节点之间的通讯是安全的。

协议无关性。隧道可以允许所有种类的帧通过。IP和非IP帧可以在IPSec隧道中传输。

路由模式。SCALANCE S可以作为路由器。可以通过该路由器,连通内网和外网。于是连接 SCALANCE S的内网就成为独立的子网。

保护设备和网段。防火墙和VPN功能可以应用在单独的设备,几个设备或整个网络中

在扁平网络中不需要响应。SCALANCE S不需要组态就可以发现内部网络的节点。这意味着当 SCALANCE S安装在已存的网络中,网络节点不需要重新组态。SCALANCE S发现这些内部节点, 而不能被发现的内网节点需要组态。

SCALANCE S上有2个RJ45端口,其中Port1红色标记的用于连接外部网络,而Port2绿色标记的用于连接内部网络。内部网络的节点是受保护的。



第二章 DHCP 服务器

2.1 DHCP 概述

DHCP 是 Dynamic Host Configuration Protocol 之缩写,它的前身是 BOOTP,即"动态主机配置协议"。

BOOTP 原本是用于无盘主机连接的网路上面的,网路主机使用 BOOTROM 而不是磁碟起动并 连接上网路,BOOTP 则可以自动地为那些主机设定 TCP/IP 环境。但 BOOTP 有一个缺点:您在设 定前须事先获得客户端的硬件地址,而且,与 IP 的对应是静态的。换而言之,BOOTP 非常缺乏" 动态性",若在有限的 IP 资源环境中,BOOTP 的一对一对应会造成非常可观的浪费。

DHCP 可以说是 BOOTP 的增强版本,它分为两个部份:一个是服务器端,而另一个是客户端。 所有的 IP 网路设定资料都由 DHCP 伺服器集中管理,并负责处理客户端的 DHCP 要求;而客户端 则会使用从伺服器分配下来的 IP 环境资料。比较起 BOOTP,DHCP 透过"租约"的概念,有效且动 态的分配客户端的 TCP/IP 设定,而且,作为兼容考量,DHCP 也完全照顾了 BOOTP Client 的需求。

SCALANCE S 可以作为内部网络的 DHCP 服务器,这样 IP 地址自动分配给内部网络的设备。IP 地址的分配可以来自于组态的地址池中,也可以给某一设备分配一个固定的 IP 地址。默认的租约为 2 天。

2.2 DHCP 组态



网络组态由两台主机 Host1 和 Host2 分别与 SCALANCE S 的端口 1 (External) 和端口 2

(Internal)相连。其中 Host1 用于配置 SCALANCE S。而 SCALANCE S 给 Host2 动态分配 IP 地址。

在配置 SCALANCE S 之前需要配置 Security Configuration Tool(简称 SCT)软件 V2.1 版本。

序号	组态步骤
1	打开 SCT,点击新建项目图标 🗋 此时弹出新建项目的用户信息,根据需要建立用户名和密
	码。这里用户名和密码均为 s。点击 OK 按钮结束。
	New administrator User Name Password * Password confirmation OK Cancel
2	对于 Type,点击下拉菜单,选择要操作的 SCALANCE S,这里使用 SCALACNE S612 V2 版本。
	在 IP Address ext 和 Subnet Mask ext 中给 SCALANCE S612 的外网 IP 地址和子网掩码为
	192.168.0.1 和 255.255.255.0。最后把 SCALANCE S612 上的 MAC 地址输入到 MAC Address
	中。
	Security Configuration Tool [Configuration1 C:\Program Files\SIEMENS\Security_Configuration_Tool\Projects\Configuration1\] Project Edit Insert Transfer Wew Options Help Image: Security Configuration Tool [Configuration1 C:\Program Files\SIEMENS\Security_Configuration_Tool\Projects\Configuration1\] Project Edit Insert Transfer Wew Options Help Image: Security Configuration Tool [Configuration1 C:\Program Files\SIEMENS\Security_Configuration_Tool\Projects\Configuration1\] Image: Security Configuration Tool [Configuration1 C:\Program Files\SIEMENS\Security_Configuration_Tool\Projects\Configuration1\] Project Edit Insert Transfer Wew Options Help Image: Security Configuration Tool [Configuration1 C:\Program Files\SIEMENS\Security_Configuration_Tool\Projects\Configuration1\] Image: Security Configuration Tool [Configuration1 C:\Program Files\SIEMENS\Security_Configuration_Tool\Projects\Configuration1\] Image: Security Configuration Tool [Configuration1 C:\Program Files\SIEMENS\Security_Configuration_Tool\Projects\Configuration1\] Image: Security Configuration Tool [Configuration Tool\Projects\Configuration Tool\Projects\Co
3	点击 View 菜单,选择高级模式 Advanced Mode。
	Security Configuration Tool [Configuration1 C:\Program Files\SIEMENS\Security_Configuration_Tool\Projects\Configuration1\] Project Edk Insert Iransfer Wew Options Help Advanced Mode Ctrl+E Offline Ctrl+Shift+D Opline Ctrl+Shift+D Opline Ctrl+D 192.168.0.1 255.255.255.0 08-00-06-96-9A-E7
	Ready Current User: s Role: Admin Standard Mode Offline > 하나소畄니 (************************************
	区旳会评冚一个警古刈冚性,掟亦一旦选拴局级俣玌,符个会切్四体准俣玌。 │

	Security Module Engineering
	Do you want to change to advanced mode? Warning: If you make changes in advanced mode, you cannot return to standard mode!
	<u>Yes</u> <u>No</u>
4	双击模块图标或者在菜单 Edit 中选择属性 Property 选项。弹出模块属性对话框。该模式是
	SCALACNE S 的高级模式。
	Module Properties - Module 1
	Network The Firewall Settings 🖼 SSL Certificate 🎨 Time Synchronization 🖓 Logging 👼 Nodes 📽 DHCP-Server 🚱 Routing Modus
	C activate DHCP
	MAC Address ClientID IP Address
	Add Remove
	dynamic IP Addresses:
	Start End
	OK Cancel Help
5	在模块属性对话框中,使能 DHCP 属性。在动态 IP 分配栏中分配 192.168.0.10 的起始地址以及
	192.168.0.99 的结束地址,这个地址段需要与 SCALANCE S 的 IP 地址处于同一网段。这里也可
	以给设备根据 MAC 地址来设置固定的 IP 地址,这里保持默认。租约默认为 2 天。点击 OK 按钮
	结束。

♥ VPN 動 Routing Modus ♥ activate DHCP static IP Addresse: MAC Addresse Add Bemove dynamic IP Addresse: Stat 192168.0.10 End 192.168.0.99 OK Cancel Heb Add Remove dynamic IP Addresse: Stat 192.168.0.10 End 192.168.0.99 OK Cancel Heb Add Remove OK Stat 192.168.0.10 End 192.168.0.10 End 192.168.0.30 Add Remove OK Cancel Heb Stat State 192.168.0.10 State 192.168.0.10 State State State State State State State State	✓ vrn 動 Routing Modus ● DHCP-Server ✓ activate DHCP tatic IP Addresse: ● MAC Address ClientID IP Addresse Add Remove dynamic IP Addresses:	Network	Firewall Settings	SSL Certificate	Time Synchronization	Logging	🖫 Nodes
▼ activate DHCP static IP Addresse: MAC Addresse: Add Pemove dynamic IP Addresse: Start 192168.0.10 End 192168.0.39 CK Cancel Help Rat工具栏上的保存图标 ■ 保存该项目。设置 Host1 的 IP 地址 192.168.0.3。点击工具和 可载图标。下载美国到 SCALANCE S612 中,直到提示下载成功。可以点击 Detail<<按钮系	✓ activate DHCP static IP Addresse: MAC Address ClientID Add Remove dynamic IP Addresse: Stati Stati 192168.010 End 192168.039 OK Cancel Heb Ratic LP Addresse: Stati 192168.010 End 192168.039 OK Cancel Heb Ratic LP Addresse: Stati 192168.010 End 192168.039 OK Cancel Heb Ratic LP Addresse: Stati 192168.030 Grade IP Addresse: OK Cancel Heb Ratic LP Addresse: Stati IP Addresse: IP Addresse: IP Addresse: IP Addresse: IP Addresse: IP Addresse:			Bouting M	ndus	DHCP-Serv	er
Add Remove dynamic IP Addresses: Start 192.168.0.10 End 192.168.0.99 OK Cancel Help 成击工具栏上的保存图标 保存该项目。设置 Host1 的 IP 地址 192.168.0.3。点击工具和 F载图标。下载 193 SCALANCE S612 中,直到提示下载成功。可以点击 Detail<<按钮系 蒙详细状态。如果在 SCALANCE S 中有先前的项目 需要通过背板按钮复位该模块。	Add Remove dynamic IP Addresses:	activate DHCP static IP Addresses: MAC Address	ClientID	IP Address			
dynamic IP Addresses: Start 192.168.0.10 End 192.168.0.99 OK Cancel UK Cancel Help 点击工具栏上的保存图标 保存该项目。设置 Host1 的 IP 地址 192.168.0.3。点击工具存的下载图标。下载 Statt 193.168.0.10	dynamic IP Addresses: Start 192.168.0.10 End 192.168.0.99 OK Cancel UK Cancel Help 点击工具栏上的保存图标 只要你有你的问题。 公置 Host1 的 IP 地址 192.168.0.3。点击工具结构下载图标。下载 的下载图标。下载 193 SCALANCE S612 中,直到提示下载成功。可以点击 Detail<<<按钮系示载详细状态。如果在 SCALANCE S 中有先前的项目,需要通过背板按钮复位该模块。		Add	Remove			
□K Cancel Help 点击工具栏上的保存图标 🕞 保存该项目。设置 Host1 的 IP 地址 192.168.0.3。点击工具 的下载图标。下载 鈍 到 SCALANCE S612 中,直到提示下载成功。可以点击 Detail<<按钮系 下载详细状态。如果在 SCALANCE S 中有先前的项目 需要通过背板按钮复位该模块。		dynamic IP Addresses:					
点击工具栏上的保存图标	点击工具栏上的保存图标 🔚 保存该项目。设置 Host1 的 IP 地址 192.168.0.3。点击工具 的下载图标。下载 ┿╡到 SCALANCE S612 中,直到提示下载成功。可以点击 Detail<<按钮系 下载详细状态。如果在 SCALANCE S 中有先前的项目,需要通过背板按钮复位该模块。	Start 192.168.0.10	End	192.168.0.99			
的下载图标。下载 到 SCALANCE S612 中,直到提示下载成功。可以点击 Detail<<按钮系	的下载图标。下载 到 SCALANCE S612 中,直到提示下载成功。可以点击 Detail<<按钮系 载详细状态。如果在 SCALANCE S 中有先前的项目,需要通过背板按钮复位该模块。	Start 192.168.0.10	End	9 192.168.0.99	0	K Cancel	Help
「载详细状态。如果在 SCALANCE S 中有先前的项目」需要通过背板按钮复位该模块。	「载详细状态。如果在 SCALANCE S 中有先前的项目,需要通过背板按钮复位该模块。	Start 192.168.0.10	End	3 192.168.0.99	 置 Host1 的 IP 地址 19	к <u>Cancel</u> 22.168.0.3。 я	│ <u></u> 「「」」 「「」」」
		Start 192.168.0.10 京击工具栏上的伊 勾下载图标。下载	End R存图标 📘	¹ 192.168.0.99 保存该项目。设置 ANCE S612 中,正	 置 Host1 的 IP 地址 19 直到提示下载成功。可	K Cancel 22.168.0.3。点 J以点击 Detail	│ <u>Help</u> 京击工具有 <<按钮到
		Start 192.168.0.10 京击工具栏上的例 为下载图标。下载 示载详细状态。如	End R存图标 日 线 🚰 王 到 SCALA D 果在 SCALAN	³ 192.168.0.99 保存该项目。设置 ANCE S612 中,正 ICE S 中有先前的 ³	 置 Host1 的 IP 地址 19 重到提示下载成功。可 页目,需要通过背板打	K Cancel 22.168.0.3。点 J以点击 Detail 安钮复位该模块	」 気击工具机 <<按钮察 央。
		Start 192.168.0.10	End 保存图标 🔒 成美国到 SCALA D果在 SCALAN	3 132.168.0.99 保存该项目。设置 ANCE S612 中,正 ICE S 中有先前的J	■ 目 Host1 的 IP 地址 19 到提示下载成功。可 可目,需要通过背板打	K Cancel 22.168.0.3。点 J以点击 Detail 安钮复位该模块	」 <u>Help</u> 気击工具和 <<按钮努 央。

Module Name:	Module1					
IP Address:	192.168.0.1		MAC Addres	s: 08-00-06	96-9A-E7	_
	✓ Logon as	current user				-
	Start	Abort	Details <<	Close		
Lun Uton 1 Se	curity Confi	euration T	ool 🕅			
https://192.1		Balacion				-
https://192.1 : Se	i) Transf	fer finished su	ccessfully			
https://192.1 : Se	<u> </u>					
https://192.1		ОК		ted		
https://192.100.0	. 	on no consi				
https://192.168.0	1:443/ dhcpd.	conf deleting				
https://192.168.0 https://192.168.0	l.1:443/ hosts di l.1:443/ machos	eleting sts deleting				
Setting local time https://192.168.0	1:443/ Reboot	. please wait 1	-2 minutes			
		, p				
 27272000 3-21-12	DM Transfer for	aishad ayaaaa	stullu			~
² /2/2008 3:21:13 设置主机 Host2	8 PM Transfer fir 的 IP 为自动	nished succes 获取。	sfully			×
Unternet Protocol General Alternate You can get IP se this capability. Oth the appropriate IP ● Use the follo IP address: Subnet mask: Default gatewar ● Use the follo Preferred DNS	PM Transfer fir 的 IP 为自动 I (TCP/IP) Prop Configuration ttings assigned auto erwise, you need to settings. address automatica wing IP address: — y: server address auto wing DNS server ac server:	nished succes 获取。 erties omatically if your n o ask your network	sfully			
ジェンション 没置主机 Host2 加ternet Protoco General Alternate You can get IP se this capability. Off the appropriate IP ①Dbtain an IP ①Use the follo IP address: Subnet mask: Default gatewa ② 0btain DNS ③ Use the follo Preferred DNS Alternate DNS	PM Transfer fir 的 IP 为自动 I (TCP/IP) Prop Configuration ttings assigned auto erwise, you need to settings. address automatica wing IP address:	nished succes 获取。 erties omatically if your n o ask your network ally consticution matically ddresses:	sfully			
2/2/2008 3:21:13 设置主机 Host2 Internet Protoco General Alternate You can get IP se this capability. Oth the appropriate IP ① Use the follo IP address: Subnet mask: Default gatewar ② Use the follo Preferred DNS Alternate DNS	PM Transfer fir 的 IP 为自动 I (TCP/IP) Prop Configuration ttings assigned auto erwise, you need to settings. address automatics wing IP address:	nished succes 获取。 erties omatically if your n o ask your network	sfully			
2/2/2008 3:21:13 设置主机 Host2 Internet Protoco General Alternate You can get IP se this capability. Off the appropriate IP ● ①Dbtain an IP ● ①Dbtain an IP ● ①Dbtain an IP ● ①Dbtain an IP ● ①get the follo IP address: Subnet mask: Default gatewa ● ①gtain DNS ● Usg the follo Preferred DNS Alternate DNS	PM Transfer fir 的 IP 为自动 I (TCP/IP) Prop Configuration ttings assigned auto erwise, you need to settings. address automatica wing IP address:	nished succes 获取。 erties omatically if your n o ask your network ally constically ddresses:	sfully			

	NDOWS\System32\cmd.exe
C: Docu	ments and Settings\Administrator>ipconfig -all
Windows	IP Configuration
	Host Name : SIMATIC
	Primary Dns Suffix :
	Node Type : Unknown
	IP Routing Enabled : No
	WINS Proxy Enabled No
	Connection-specific DNS Suffix . :
	Description
	Physical Address
	Dhcp Enabled : Yes
	Autoconfiguration Enabled : Yes
	IP Address : 192.168.0.10
	Subnet Mask
	Default Gateway :
	DHCP Server : 192.168.0.1
	Lease Obtained : 2008年2月2日 16:37:13

- 第三章 Syslog
- 3.1 Syslog 概述

Syslog 是 IP 网络中转发日志消息的标准协议。这个术语 Syslog 常常看作实际的 Syslog 协议,

以及应用或者发送 Syslog 信息的库。

Syslog 协议是一个 Client/Server 的结构: Syslog 发送者发送少于 1024 个字节给 Syslog 接收

者。接收者常常被称为 Syslogd, Syslog daeman 或者 Syslog server。Syslog 消息可以通过 UDP

或者 TCP 来发送。数据发送以纯文本结构,可以通过 SSL 进行数据加密。

Syslog 典型的用于网络系统的管理和安全审查。大多数设备和跨平台的接收者都支持 Syslog,

这样 Syslog 就可以从不同类型的系统读取日志文件到中央存储。

SCALANCE S 的日志文件可以通过组态发送到 Syslogd 上,这样可以方便的管理和诊断

SCALANCE S.

3.2 Syslog 组态

Syslog 网络组态图:



Host1 与 SCALANCE S 的端口 1 相连, IP 地址如图所示。在配置 SCALANCE S 之前需要配置 Security Configuration Tool(简称 SCT)软件 V2.1 版本。在 Syslog client 中需要安装 Syslogd,这 里安装了免费的 Kiwi syslog daemon。

序号 组态步骤 1 参考 DHCP 服务器的组态步骤到 4。双击模块图标或者在菜单 Edit 中选择属性 Property 选项。 弹出模块属性对话框。使能 Enable logging to Syslog Server 选项,设置 192.168.0.3 的 Syslog Server 的 IP 地址。点击 OK 按钮结束。 Module Properties - Module1 VPN 遺 Routing Modus 💶 DHCP-Server 🖼 SSL Certificate 🔰 🕒 Time Synchronization 💭 Logging Network Firewall Settings 🛃 Nodes Local Log Buffers Event Classes to log **Ring-Buffer** One Shot Buffer enable Event-Class Log buffer Packet Filter Events (firewall) œ. C Packet Log Audit Events 6 Audit Log Configure ... System events œ C System Log Network Syslog 192.168.0.3 Enable logging to Syslog-Server Syslog Server Module1 Module Hostname Use symbolic names in log Event Classes to log enable Event-Class assign Severity assign Facility Packet Filter Events (firewall) default default • -Audit Events default default -System Events ΟK Cancel Help 2 保存和下载项目参考 DHCP 项目的步骤 6。打开 Kiwi syslog daemon,可以看见 SCALANCE S 的 日志文件。

8 2 📖		– Display 00 (De	efault) 🔽		
Date	Time	Priority	Hostname	Message	
02-03-2008	13:14:01	Syslog.Info	192.168.0.1	FEB 03 21:14:01 syslogd: restart	

第四章 防火墙

4.1 防火墙概述

防火墙的基本任务就是控制不同信任级别的计算机网络中的数据流。所有来自于外部网络的 防护是绝对必须的。防火墙不但可以应用在Internet,也可以应用在Intranet中,特别是在重要的 工业现场局域网中。通过防火墙可以防止外部网络的非法访问和错误操作,保护PLC等现场设备 正常的运行。防火墙可以通过过滤数据包例如IP地址或端口号,监视应用层的内容以及监视外部 访问的授权等,来实现某一特定的安全策略。

SCALANCE S作为防火墙的主要作用就是防止外网非法入侵以保护内网的安全。这就意味着通 过某些组态,某些外部网络到内部网络的数据流才允许通过。所有处于内网的节点受SCALANCE S 防火墙的保护。SCALANCE S支持状态包检测,非IP包的过滤(2层数据帧),带宽限制等等实现 防火墙的功能。

4.2 防火墙组态



主机 Host1 与 SCALANCE S 的端口 1 相连,西门子交换机 SCALANCE X414-3E 与 SCALANCE S 的 端口 2 相连。这时 Host1 处于外网,而 SCALANCE X414-3E 处于内部网络。默认 SCALANCE S 是 一个防火墙,阻止任何外部数据访问内部网络,只能通过一系列的组态允许某些外部数据访问内 部网络。通过设置,Host1 可以使用 PST 工具扫描到 SCALANCE X414-3E,在 Host1 中可以通过 IE 浏览器浏览 SCALANCE X414-3E 的 Web。

序号	组态步骤
1	参考 DHCP 服务器的组态步骤到 2。双击模块图标或者在菜单 Edit 中选择属性 Property 选项。
	弹出模块属性对话框。该模式是 SCALACNE S 的标准模式。
	Module Properties - Module1
	🗎 Network 🗰 Firewall Settings 🕼 Time Synchronization 🔀 Routing Modus
	Configuration Tunnel communication only Allow access to NTP server from internal to external network
	Allow IP traffic from internal to Allow SiClock time messages from external network
	Allow IP traffic with S7 protocol from Internal to external network Internal to external network
	Allow access to DHCP server from Allow configuration of nodes via DCP
	IP Logging MAC Log Settings
	Log tunneled packets I Log passed packets
	Log blocked incoming packets I Log blocked incoming packets
	Log blocked outgoing packets I Log blocked outgoing packets
	OK Cancel Help
	保存和卜载默认坝目参考 DHCP 坝目的步骤 6。
2	按照网络连接,在 Host1 中打开 PST 工具,扫描网络中的设备。结果可以发现仅有 SCALANCE
	S _o
	🖻 Primary Setup Tool - Broadcom NetXtreme 57xx Gigabit Controller - Packet Scheduler Minipo 🔲 🗖 🔀
	Network Module Settings 2
	General information General information
	Device name : Scalance S 6xx
	通过 IE 浏览器不能打开 192.168.0.100 的 Web 页面。

	Cannot find server - Microsoft Internet Explorer
	File Edit View Favorites Tools Help
	🕜 Back - 🕥 - 🖹 📓 🏠 🔎 Search 📌 Favorites 🤣 🔗 - 🍑 💭 🗒 🦓 🦓
	Address 🗿 192.168.0.100
	The page cannot be disp The page you are looking for is currently ur site might be experiencing technical difficult to adjust your browser settings.
3	打开 SCALANCE S 标准属性的对话框选择 Firewall setting 栏,使能 Allow configuration of
	nodes via DCP。点击 OK 按钮结束。 Module Properties - Module1
	🗎 Network 🗰 Firewall Settings 🎼 Time Synchronization 🗒 Routing Modus
	Configuration Cunnel communication only Allow access to NTP server from internal to external network
	Allow IP traffic from internal to Allow SiClock time messages from external network
	Allow IP traffic with S7 protocol from Internal to external network Internal to external network
	□ Allow access to DHCP server from □ Allow configuration of nodes via DCP
	IP LoggingMAC Log Settings
	Log tunneled packets Log passed packets
	Image: Log blocked incoming packets Image: Log blocked incoming packets
	Log blocked outgoing packets
	OK Cancel Help
4	选择高级模式,具体方式参考 DHCP 项目的 3 和 4。点选 Firewall settings 栏。点击 IP Serive
	Definitions按钮。在 TCP 服务中,点击按钮 Add IP Service 增加一个 IP 服务 Service0,修改名
	字为 HTTP,目的端口号设置为 80。该端口号是 HTTP 服务的端口号。然后点击 OK 结束。

	Name		Protocol	Source Port	Target Por	t	
	HTTP		top	*	80		
	1			1	ID Card	1	
		-	Add IP Service	Hemo	ve IP Service		
				Ť	ПK	L Cance	
						-1897 -	
5	在 Firewall Allow,方向 IP,这里为	settings 高级属 向为外部到内部 默认。点击 OK	性对话框中,点 External->Intern 按钮结束。	击 Add Rule i al,服务为 F	按钮,增加 HTTP。也回]一个安全]以根据需	规则,动 要设置源
5	在 Firewall Allow,方向 IP,这里为影	settings 高级属 句为外部到内部 默认。点击 OK ies - Module1	『性对话框中,点言 External->Intern 按钮结束。	击 Add Rule i al,服务为 H	按钮,增加 HTTP。也同	□一个安全: 〕以根据需	规则,动
5	在 Firewall Allow,方向 IP,这里为 Module Properti	settings 高级属 句为外部到内部 默认。点击 OK ies - Module1	『性对话框中,点 External->Intern 按钮结束。	击 Add Rule al,服务为 H Routing Modus ficate ① T	按钮,增加 HTTP。也可	□一个安全:]以根据需 n ^[2] L	规则,动 要设置源 ^{DHCP-Server}
5	在 Firewall Allow,方向 IP,这里为 Module Propertion IP Rules M	settings 高级属 句为外部到内部 默认。点击 OK ies - Module1 YPN WPN IAC Rules	3性对话框中,点 External->Intern 按钮结束。	击 Add Rule a al,服务为 H Routing Modus ficate 1 ① T	按钮,增加 HTTP。也可 ime Synchronizatio	コー个安全: J以根据需 m <u></u> りし	规则,动 要设置源 DHCP-Server .ogging
5	在 Firewall Allow,方向 IP,这里为影 Module Properti IP Rules M Action	settings 高级属 句为外部到内部 默认。点击 OK ies - Module1 《 VPN 《 WPN 《 WPN 《 CRules Direction	6性对话框中,点 5 External->Intern 按钮结束。 ^{ttings}	击 Add Rule a al,服务为 H Routing Modus ficate 1 ① T	按钮,增加 HTTP。也可 ime Synchronizatio Serv	□一个安全: J以根据需 m ^劉 L	规则,动1 要设置源 DHCP-Server .ogging Bandwidth(N
5	在 Firewall Allow,方向 IP,这里为 Module Propertion IP Rules M Action	settings 高级属 句为外部到内部 默认。点击 OK ies - Module1 Set WPN WPN WPN WPN WPN CRules Direction	3性对话框中,点 External->Intern 按钮结束。	击 Add Rule al,服务为 H Routing Modus ficate ① T Destination IP	按钮,增加 HTTP。也可 ime Synchronizatio	□一个安全: J以根据需 m │ 卿 L ice	规则,动作 要设置源 DHCP-Server .ogging
5	在 Firewall Allow,方向 IP,这里为影 Module Properti IP Rules M Action	settings 高级属 句为外部到内部 默认。点击 OK I <mark>tes - Module1</mark> WPN WPN IAC Rules	5性对话框中,点 5 External->Intern 按钮结束。	击 Add Rule a al,服务为 H auting Modus ficate ① T	按钮,增加 HTTP。也可 ime Synchronizatio	」一个安全: J以根据需 m 卿 L ice	规则,动作 要设置源 DHCP-Server .ogging Bandwidth(N
5	在 Firewall Allow,方向 IP,这里为 Module Propertion	settings 高级属 句为外部到内部 默认。点击 OK I <mark>es - Module1</mark> I <mark>es - Module1</mark> IIE Rules Direction	3性对话框中,点 External->Intern 按钮结束。	击 Add Rule al,服务为 H Routing Modus ficate ① T	按钮,增加 HTTP。也可 ime Synchronizatio	□一个安全: J以根据需 m │ 卿 L ice	规则,动作 要设置源 DHCP-Server .ogging
5	在 Firewall Allow,方向 IP,这里为影 Module Properti IP Rules M Action	settings 高级属 句为外部到内部 默认。点击 OK ies - Module1 《VPN 《WPN 《WPN 《UPN 》Firewall Set Direction	3性对话框中,点 External->Intern 按钮结束。	击 Add Rule al,服务为 H Routing Modus ficate ① T	按钮,增加 HTTP。也可 ime Synchronizatio	□一个安全: J以根据需 m 卿 L ice	规则,动作 要设置源 DHCP-Server .ogging Bandwidth(N
5	在 Firewall Allow,方向 IP,这里为 Module Propertion	settings 高级属 句为外部到内部 默认。点击 OK Interval Set MAC Rules	3性对话框中,点 External->Intern 按钮结束。	击 Add Rule al,服务为 H Routing Modus ficate ① T	按钮,增加 HTTP。也可 ime Synchronizatio	□一个安全: J以根据需 m 卿 L ice	规则,动作 要设置源 DHCP-Server .ogging Bandwidth(N
5	在 Firewall Allow,方向 IP,这里为 Module Properto Network IP Rules M Action	settings 高级属 句为外部到内部 默认。点击 OK ies - Module1 《VPN 《WPN 《Image: Set Direction 》External->Internal 《	3性对话框中,点 5 External->Intern 按钮结束。 ttings │ 聲 SSL Certi Source IP	击 Add Rule al,服务为 H Routing Modus ficate ① T	按钮,增加 HTTP。也可 ime Synchronizatio	□一个安全: J以根据需 m 卿 L ice	规则,动作 要设置源 DHCP-Server .ogging Bandwidth(N
5	在 Firewall Allow,方向 IP,这里为 Module Propertion	settings 高级属 句为外部到内部 默认。点击 OK ies - Module1 《 YPN 《 W Firewall Set MAC Rules	3性对话框中,点 External->Intern 按钮结束。	击 Add Rule al ,服务为 H Routing Modus ficate 1 ① T	按钮,增加 HTTP。也可 ime Synchronizatio	□一个安全: J以根据需 m 卿 L ice	规则,动作 要设置源 DHCP-Server .ogging Bandwidth(N
5	在 Firewall Allow,方向 IP,这里为 Module Properto P Rules M Action	settings 高级属 句为外部到内部 默认。点击 OK ies - Module1 《VPN 《UPN 》 Firewall Set Direction 》 External->Internal 《	3性对话框中,点 External->Intern 按钮结束。 ◎ SSL Certi Source IP	击 Add Rule al , 服务为 H Routing Modus ficate ① T	按钮,增加 HTTP。也可 ime Synchronizatio	□一个安全: J以根据需 m 卿 L ice	规则,动 要设置源 DHCP-Server .ogging Bandwidth(N
	在 Firewall Allow,方向 IP,这里为影 Module Properti P Rules M Action	settings 高级属 句为外部到内部 默认。点击 OK ies - Module1 《 VPN 《 W Firewall Set MAC Rules	3性对话框中,点 External->Intern 按钮结束。	击 Add Rule al ,服务为 H Routing Modus ficate ① T Destination IP	按钮,增加 HTTP。也可 ime Synchronizatio	□一个安全: J以根据需 m 卿 L ice	规则,动 定要设置源 DHCP-Server .ogging Bandwidth(N
5	在 Firewall Allow,方向 IP,这里为 Module Properto P Rules M Action	settings 高级属 句为外部到内部 默认。点击 OK tes - Module1 《 VPN 《 WPN 《 Trirewall Set Direction 》 External->Internal 《	3性对话框中,点 External->Intern 按钮结束。	击 Add Rule al , 服务为 H Routing Modus ficate ① T	按钮,增加 HTTP。也可 ime Synchronizatio	□一个安全: J以根据需 m 卿 L ice	规则,动作 要设置源 DHCP-Server .ogging Bandwidth(N

14

6	保存和下载默认项目,参考 DHCP 项目的步骤 6。在 Host1 中打开	PST 工具浏览网络。可以看
	见 SCALANCE X414-3E。	
	Primary Setup Tool - Broadcom NetXtreme 57xx Gigabit Controller - Packa Network Module Settings 2 ▲	et Scheduler Minipo 🖃 🗖 🗙
	通过 IE 浏览	
	SCALANCE X-400 WEB Management - Microsoft Internet Explorer File Edit View Favorites Tools Help	
	Search Search	<mark>,</mark> (2, 48
	SIEMENS	Automation & Drives
	Console Support	SIMATIC NET
	Authorization	
	Liser name: admin	
	Password:	
	Logon using a secure HTTPS connection	

第五章 虚拟专用网络

5.1 VPN 概述

VPN即虚拟专用网 (Virtal Private Network),是一条穿过混乱的公用网络(非安全的网络)的 安全、受保护的、稳定的隧道。通过对网络数据的封包和加密传输,在一个公用网络(通常是因 特网)建立一个临时的、安全的连接,从而实现在公网上传输私有数据、达到私有网络的安全级 别。通常,VPN是对企业内部网的扩展,通过它可以帮助远程用户、公司分支机构、商业伙伴及 供应商同公司的内部网建立可信的安全连接,并保证数据的安全传输。而对于工业网络,VPN可 以是用安全机制来保障设备之间数据交换的机密型(Confidentiality),真实可靠行

(Authentication),完整性(Integrity)严格的访问控制。这样就建立了一个逻辑上虚拟的私有 网络。VPN提供了一个经济有效的手段来解决通过公用网络安全的交换私有信息。 在建立VPN时,需要VPN Server和VPN Client,并且以成对的方式出现。例如,可以通过两个 SCALANCE S建立VPN通道,也可以利用Softnet Security Client软件实现PC与SCALANCE S之间建立 VPN通道。这样SCALANCE S的内网以及PC都是安全的网络。

Copyright © Siemens AG Copyright year All rights reserved

> VPN的隧道技术本质上是封装技术,所谓封装技术就是原始数据包通过某一层时,额外增加 了包头,这样完成从一种协议的完整报文没有变化的生成另外一种协议的报文。

SCALANCE S使用IPSec协议的隧道模式实现VPN的隧道。IPSec是在发展IPv6时创建的,是IPv6 的一部分。其工作在ISO/OSI的网络层,即第3层。IPSec协议把多种安全技术集合到一起,可以建立 一个安全、可靠的隧道。IPSec是一种基于点到点的连接,实现安全全联盟(SA Security Association)的连接。IPSec是在IP网络上保证安全通信的开放标准框架,IPSec实际上是一套协议 包而不是单个的协议,它在IP层提供数据源验证、数据完整性和数据保密性。其中比较重要的有 RFC2409 IKE(Internet Key Exchange)互连网密钥交换、RFC2402 AH(Authentication Header) 验证包头、RFC2406 ESP (Encapsulating Security Payload 封装安全载荷) 加密数据等协议。

IPSec通过AH和ESP这两个安全协议来实现数据源验证、数据完整性和数据保密性的目标,并 且还可以通过IKE为IPSec提供了自动协商交换密钥、建立和维护安全联盟SA的服务,以简化IPSec 的使用和管理。AH是包头验证协议,主要提供的功能有数据源验证、数据完整性校验和防报文重 放功能;然而,AH并不加密所保护的数据报。ESP是封装安全载荷协议,它除提供AH协议的所有 功能之外(但其数据完整性校验不包括IP头),还可提供对IP报文的加密功能。AH和ESP可以单独 使用,也可以同时使用。对于AH和ESP,都有两种操作模式:传输模式和隧道模式。SCALANCE S 应用VPN安全策略时仅使用ESP安全协议。

IKE使用了两个阶段为IPSec进行密钥协商并建立安全联盟:第一阶段,通信各方彼此间建立了 一个已通过身份验证和安全保护的通道,此阶段的交换建立了一个安全联盟,称为IKE SA;第二 阶段,用第一阶段所建立的安全通道为IPSec协商安全服务,即为IPsec协商具体的安全联盟,建立 IPSec SA,而IPSec SA用于最终的IP数据安全传送。

IPSec SA可以通过手工配置的方式建立,但是当网络中节点增多时,手工配置将非常困难,而 且难以保证安全性。这时就要使用IKE自动地进行安全联盟建立与密钥交换的过程。IKE协议为

16

IPSec提供了自动协商交换密钥、建立安全联盟的服务,以简化IPSec的使用和管理。IKE具有一套 自保护机制,可以在不安全的网络上安全地分发密钥、验证身份、建立IKE安全联盟。

DH(Diffie-Hellman)交换及密钥分发。Diffie-Hellman算法是一种公共密钥算法。通信双方 在不传送密钥的情况下通过交换一些数据,计算出共享的密钥。加密的前提是交换加密数据的双 方必须要有共享的密钥。IKE的精髓在于它永远不在不安全的网络上直接传送密钥,而是通过一系 列数据的交换,最终计算出双方共享的密钥。即使第三者(如黑客)截获了双方用于计算密钥的 所有交换数据,也不足以计算出真正的密钥。完善的前向安全性(Perfect Forward Secrecy, PFS)。PFS是一种安全特性,指一个密钥被破解,并不影响其他密钥的安全性,因为这些密钥间 没有派生关系。PFS是由DH算法保障的。

身份验证。身份验证确认通信双方的身份。对于pre-shared key验证方法,验证字用来作为一个输入产生密钥,验证字不同是不可能在双方产生相同的密钥的。验证字是验证双方身份的关键。

身份保护。身份数据在密钥产生之后加密传送,实现了对身份数据的保护。

在RFC2409中规定,IKE第一阶段的协商可以采用两种模式:主模式(main mode)和野蛮模式(aggressive mode)。两者的主要区别在于野蛮模式不提供身份保护。SCALANCE S可以使用 IKE自动协商建立IKE SA。并可以根据需要的网络环境选择主模式或野蛮模式。

安全联盟是IPSec的基础,也是IPSec的本质。SA是通信对方对某些要素的约定,例如,使用哪种协议(AH、ESP还是两者结合使用)、协议的操作模式(传输模式和隧道模式)、加密算法 (DES和3DES)、特定流中保护数据的共享密钥以及密钥的生存周期等。

IPSec SA安全联盟是单向的,在两个对等体之间的双向通信,最少需要两个安全联盟来分别对 两个方向的数据流进行安全保护。安全联盟具有生存周期。生存周期的计算包括两种方式:以时 间为限制,每隔指定长度的时间就进行更新;以流量为限制,每传输指定的数据量(字节)就进 行更新。SCALANCE S使用时间或者流量来更新IPSec SA。

AH和ESP都能够对IP报文的完整性进行验证,以判别报文在传输过程中是否被篡改。验证算法 的实现主要是通过杂凑函数,杂凑函数是一种能够接受任意长的消息输入,并产生固定长度输出 的算法,该输出称为消息摘要。IPSec 对方计算摘要,如果两个摘要是相同的,则表示报文是完 整未经篡改的。一般来说IPSec使用两种验证算法:MD5(Message Digest Version 5)通过输入 任意长度的消息,产生128bit的消息摘要。SHA-1通过输入长度小于2的64次方比特的消息,产生 160bit的消息摘要。SHA-1(Secure Hash Algorithm 1)的摘要长于MD5,因而是更安全的。在 IPSec SA阶段,SCALANCE S可以设置MD5或者SHA-1。

ESP能够对IP报文内容进行加密保护,防止报文内容在传输过程中被窥探。加密算法实现主要 通过对称密钥系统,它使用相同的密钥对数据进行加密和解密。一般来说IPSec使用两种加密算 法:DES(Data encryption standard)使用56bit的密钥对一个64bit的明文块进行加密。3DES (Special triple DES)使用三个56bit的DES密钥(共168bit密钥)对明文进行加密。3DES具有更 高的安全性,但其加密数据的速度要比DES慢得多。在IPSec SA阶段,SCALANCE S除了可以使用 DES或3DES进行数据加密,还可使用AES(Advanced Encrypting Standard)的方法进行加密。 5.2 VPN 组态



^{192.168.0.3}

Host1 与交换机 SCALANCE X414-3E 相连, 2 个 SCALANCE S 的外部网络端口 1 分别与 SCALANCE

X414-3E相连。	2个 SCALANCE S的内部网络端口分别与主机 Host2和 Host3 材	相连。
------------	--	-----

序号	组态步骤
1	新建项目用户名和密码均为 vpn,具体组态参考 DHCP 组态步骤。在项目中加入两个安全模块

	Becurry configuration root Project Edit Insert Iransfer View Diffine View Module1 Module2 VPN Groups	vpn C: VProgram Files Options Help er Name Type Module1 S612 V2 Module2 S612 V2	SIEMENSUS County IP Address ext. 192.168.0.1 192.168.0.2	Configuration_ToolVProje Subnet Mask ext. IP Add 255.255.255.0 255.255.0	ects\Configuration1\vpn\] ress int. Subnet Mask int. Defa	ault Router MAC Address 08-00-06-96-94 08-00-06-96-94
	Ready			Current User: v	/pn Role: Admin	Standard Mode Offline
2	在左侧栏内,右键点	転 VPN Group n Tool [vpn C:)	os,插入一~ Program FilesV	个新组。或点击 SIEMENS\Security_(古工具栏按钮 <mark>希</mark> 。 Configuration_Tool\Proje	ectsICo 💶 🗖 🗙
			- 9 9			
	Offline View	Group Name		Authentication	Group membership unti	il Comment
	Copy Paste					
	Ready Rename 就认为 Group1。		Current User: v	pn Role: Admin	Standard	Mode Offline 9
	Ready Rename Rename 就认为 Group1。	n Tool [vpn C:V	Current User: v Program Files)	pn Role: Admin	Standard Configuration_Tool\Proje	Mode Offline 9
	Ready Rename Rename Rename 默认为 Group1。	n Tool [vpn C:V er View Options He F 4 (1)	Current User: v Program Files) elp 9 °a	pn Role: Admin	Standard Configuration_Tool\Proje	Mode Offline 9
	Ready Rename Rename Rename 就认为 Group1。 新 Security Configuratio Project Edit Insert Iransf D 译 图 图 图 X	n Tool [vpn C:V ⁱ er View Options He Group Name	Current User: v Program Files elp 2 2 1	pn Role: Admin SIEMENS\Security_	Standard Configuration_Tool\Proje Group membership unt	Mode Offline 9 ects\Co = [])
	Ready Rename Rename 默认为 Group1。 Security Configuratio Project Edit Insert Transf DIELE (Insert Transf DIELE (Inse	n Tool [vpn C:V er View Options He Group Name	Current User: v Program Files) elp 2 2 2	pn Role: Admin SIEMENS\Security Authentication Certificate	Standard Configuration_Tool\Proje	i Mode Offline 9
	Ready Rename Rename 默认为 Group1。 Security Configuratio Project Edit Insert Iransf D 定 图 图 图 图 0 Offline View Offline View Offline View Offline View Offline View Offline View Offline View Group1	n Tool [vpn C:V er View Options He Group Name Group 1	Current User: v Program Files elp	pn Role: Admin SIEMENS\Security_ Authentication Certificate	Standard Configuration_Tool\Proje	Mode Offline 9
	Ready Rename Rename 默认为 Group1。 Security Configuratio Project Edit Insert Transf DEF W Offline View Offline View All Modules Module1 Module2 WPN Group1 Ready	n Tool [vpn C:V er View Options He Group Name	Current User: v Program Files P P P P Current User: v	pn Role: Admin SIEMENS\Security Authentication Certificate pn Role: Admin	Standard Configuration_Tool\Proje Group membership unt Standard	Mode Offline 9
3	Ready Rename 默认为 Group1。 Security Configuratio Project Edit Insert Iransf DIFINE View All Modules Module1 Module2 WIN Group1 Ready 然后在左侧栏内,用	n Tool [vpn C: V er View Options He Group Name 子Group1	Current User: v Program Files P P P P P P P P P P P P P P P P P P P	pn Role: Admin SIEMENS\Security_ Authentication Certificate pn Role: Admin codule2 到新建的	Standard Configuration_Tool\Proje Group membership unt Standard 的 VPN Group1 中。	Mode Offline 9 ects\Co () () til Comment

Project Edit Insert Iran	nsfer <u>View Options H</u> elp		
Offline View	Num Name Authentica Group membe	rship until Type	C
E 📄 All Modules	Module1(Shortcut) Certificate 2/13/2037	S612 V2	
Module2	and 2 Module2(Shortcut) Certificate 2/13/2037	S612 V2	
a a choop?		-	-
Ready	Current User: vpn Role: Admin	Standard Mode Offline	9
Security Configuration Project Edit Insert Trans	ion Tool [vpn C:\Prop Sfer View Options Help Certificate valid until:	tion_Tool\Projects\Co 🔳 🗖	
Security Configuration Project Edit Insert Trans DEP DE DE DE X Offline View Def De View De All Modules	ion Tool [vpn C:\Pro Certificate Validity X sfer View Options Help Certificate valid until: 13.07.2036 Group Name July, 2036 Sun Mon Tue Wed Thu Fri Sat Sun Mon Tue Wed Thu Fri Sat Sun Mon Tue Wed Thu Fri Sat	tion_Tool\Projects\Co [] membership until Comment 036	
Security Configuration Project Edit Insert Trans DEE E E E E E Offline View Offline View Module1 Module2 WVPN Groups Group1	Certificate Validity Sfer View Options Help Group Name July. 2036 Group 1 (Shortcut) July. 2036 Sun Mon Tue Wed Thu Fri Sat 23 30 1 2 3 Image: Strain Strai	tion_Tool\Projects\Co	
Security Configuration Project Edit Insert Trans Confline View All Modules Module1 Module2 WPN Groups Group1	Certificate Validity Sfer View Options Help Group Name July. 2036 Group Name July. 2036 Group Name July. 2036 Output July. 2036 July. 2036 July. 2036 July. 2036 July. 2036 July. 2036 July. 2036 July. 2037 July. 2036 July. 2038 July. 2036 July. 2036 July. 2036 July. 2037 July. 2036 July. 2038 July. 2038 July. 2038 July. 2038 July. 2038 July. 2038 July. 2038 July. 2038 July. 2038 July. 2038<	tion_Tool\Projects\Co	
Security Configuration Project Edit Insert Trans Diffline View Offline View Module1 Module2 WPN Groups Ready Ready	Certificate Validity Set Wiew Options Help Group Name July. 2036 Group Name July. 2036 Group Name July. 2036 Unit of the set o	tion_Tool\Projects\Co membership until Comment 036 Standard Mode Offline	
Security Configuration Project Edit Insert Trans Diffine View Offline View Module1 Module2 W VPN Groups Group1 Ready 电子证书的验证方:	ter View Options Help Group Name Group 1(Shortcut) Certificate Valid until: 13.07.2036 Univ. 2036 Univ. 203	tion_Tool\Projects\Co 。 membership until Comment 036 Standard Mode Offline 择 View 菜单下的 Advan	ced
 Security Configuration Project Edit Insert Trans Diffine View Offline View Module1 Module2 VPN Groups Group1 Ready 电子证书的验证方: Mode。双击 VPN Context	ion Tool [vpn C: Vro sfer View Options Help Group Name Certificate Validity Image: Certificate Valid until: 1307.2036 1307.2036 1307.2036 Group Name 1307.2036 1011 Sum Mon Tue Wed Thu Fri Sat 29 30 1 2 3 4 5 29 30 1 2 3 4 5 5 6 7 8 9 10 11 12 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 5 7 8 9 Current Today: 2/13/2008 difficate valid until: St非常安全,也可以使用预制共享密钥验证。选 Groups 下的右侧栏的 Goup1 图标,弹出 Group J	tion_Tool\Projects\Co 。 membership until Comment 036 Standard Mode Offline 择 View 菜单下的 Advan 属性。选择预制共享密钥)× ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・

ght © Siemens	opyright year	thts reserved
Copyright	AG Copy	All rights

Preshared Key		C Certi	ficate		
Key: 7BI7KCKfl	huCtH-ZR	Name:	PDCFA-G3A54		
			New	Import	Properties
Advanced Settings Pha	se 1				
IKE Mode:	Main	-			
Phase 1 DH Group:	Group2	•			
SA Lifetype:	Time	-	SA Life:	2500000	
Phase 1 Encryption:	3DES-168	•	Phase 1 Authentication:	SHA1	<u>_</u>
Advanced Settings Pha	se 2				
SA Lifetype:	Time	•	SA Life:	2880	
Phase 2 Encryption:	3DES-168	-	Phase 2 Authentication:	SHA1	•
	Perfect Forward	Secrecy			
			Г	014	
			L	UK	Lancel
时,项目 VPN的	勺安全联盟的验 t <mark>ion Tool [vpn C</mark> ansfer ⊻jew _options < _ ■ 品職 ை	证方式通〕 :\Program Fil ^{Help} 『 [©] [©] ■	호 Preshared Key 的	D方式。 onfiguration	_Tool\Projects\Co
Project Edit Insert Ira	provide and the second s			Group mer	mbership until 🛛 Cor
Project Edit Insert Inc D B B B B B B B B B B B B B B B B B B B	Group Name		Authentication	1	
Project Edit Insert Ins Diffine View Control Global FW-Rulesets All Modules Module1 Module2 Module2 Module2	Group Name		Authentication Preshared		
Project Edit Insert Ira Diffine View Colobal FW-Rulesets All Modules Module1 Module2 OVPN Groups Group1	Group Name		Authentication Preshared		

Module Name	Status
Module1	Changed
Module2	Changed
	C. (
M Logon as current	User Select All
Show only chang	ed modules Deselect All
	Processing: Module1
Start	Skip Abort Details << Close
2/13/2008 3:21:24 PM 2/13/2008 3:21:24 PM Starting GetIP Establishing connection Uploading version https://192.168.0.1:443	Transfer started Module1 Transfer started //////////////////////////////////
2/13/2008 3:21:24 PM 2/13/2008 3:21:24 PM Starting GetIP Establishing connection Jploading version https://192.168.0.1:443 : Section was https://192.168.0.1:443	Transfer started Module1 Transfer started Proi_info.txt File transfer started transferred successfully V0.0.0.2 (ip. conf File transfer started) (interview of the transfer started) (interview of the transfer started)
2/13/2008 3:21:24 PM 2/13/2008 3:21:24 PM Starting GetIP Establishing connection Uploading version https://192.168.0.1:443 : Section was https://192.168.0.1:443	Transfer started Module1 Transfer started Proi_info.txt File transfer started transferred successfully V0.0.0.2 proof File transfer started Ites
2/13/2008 3:21:24 PM 2/13/2008 3:21:24 PM Starting GetIP Establishing connection Jploading version https://192.168.0.1:443 : Section was https://192.168.0.1:443 : 意下载状态。 wnload To All Modu Module Name ☑ Module1	Transfer started Module1 Transfer started Weights the transfer started transferred successfully V0.0.0.2 Ites Status Download OK
2/13/2008 3:21:24 PM 2/13/2008 3:21:24 PM Starting GetIP Establishing connection Jploading version https://192.168.0.1:443 : Section was https://192.168.0.1:443 : Section was buttops://192.168.0.1:443 : Section was ttps://192.168.0.1:443 : Section was Mathematical Section was ttps://192.168.0.1:443 :	Transfer started Module1 Transfer started B/ proj_info.txt File transfer started transferred successfully V0.0.0.2 B/ ip. conf File transfer started Ites Status Download OK Download OK
2/13/2008 3:21:24 PM 2/13/2008 3:21:24 PM 5tarting GetIP Establishing connection Jploading version https://192.168.0.1:443 : Section was https://192.168.0.1:443 : Section was https://192.168.0.1:443 : Section was nttps://192.168.0.1:443 Module Name Module Name Module Name Module Name Module 1 Module 2 用 Ping 测试,利用	Transfer started Module1 Transfer started Proj_info.txt File transfer started transferred successfully V0.0.2 Proventional started transferred successfully V0.0.2 Provide the transfer started The transfer started Status Download OK Download OK Download OK Download OK

pyright © Siemens	G Copyright year	II rights reserved
Cop	AG	Ψ

All Modules Module1 Module2 VPN Groups Group1	Num Heachab	e Name Module1(Short Module2(Short	cut) P cut) P	uthentica	Group men	nbership unti	I I IVDE
Modules Module1 Module2 VPN Groups Group1	ang 1 Yes	Module1(Short Module2(Short	cut) P cut) P	'reshared			0040
VPN Groups	nu z tes	Module2(Short	cuty P				S612
CVPN Groups				resnared			5012
Circup1							
<							
	<)	
Ready	0	Current User: vpn R	ole: Admin		Adv	anced Mod	e Onlin
							1 Section 1
				H.O.(11			
上 句计演口士 译	百分子 山立	井占 ハハーヘー・・	1 的 译 印	++太/= 6	1		
5、 21 21 泥口芯、 55	如仇仄心、内部	ア点。IVIOQUIE	的迪讯	(仄心信足	0		
Module1 [Online View]			38				
Status Date and Time System I	og Audit Log Packet Fil	er Log Communication S	tatus Internal Nr	ndes			
oradio Date and Time Oyotom E		ion Eog	Internative	odee [
Known Scalance S Devices							
Kilowin ocalarice o Devices							
Name IP Addres	s Known By	Tunnel Status					
	12 configured	enabled					
To de state he bie de la de	03 160 0 3	Karavan Dur					
Endpoints behind:	92.168.0.2	Known By:	configured	1			
IP MAC	Kno	wn By Subne	t ID/Subnet mask				
A 192 169 0 5 09:00:0	6·90·BA·AD lear	ned					
	0.00.00.00						
132.100.0.3 00.00.0		neu					
132.100.0.3		neu					
Properties of tunnel to:	192 168 0 2						
Properties of tunnel to:	192.168.0.2	nounti Authoptic-ti		Putos Elapos d	Coff Eucire	Hard Eurica	Coff Euro
Properties of tunnel to: Status Source	192.168.0.2 Destination E	ncrypti Authentication	SPI [Bytes Elapsed	Soft Expira	Hard Expira	Soft Exp
Properties of tunnel to: Status Source enabled 192,188.0.1	192.168.0.2 Destination E 192.168.0.2 3	ncrypti Authentication DES HMAC-SHA1	SPI 01a51041	Bytes Elapsed 38408	Soft Expira	Hard Expira	Soft Exp
Properties of tunnel to: Status Source enabled 192,168,0,1 enabled 192,168,0,2	192.168.0.2 Destination E 192.168.0.2 3 192.168.0.1 3	ncrypti Authentication DES HMAC-SHA1 DES HMAC-SHA1	SPI 01a51041 d9763ae1	Bytes Elapsed 38408 9216	Soft Expira 154576 154576	Hard Expira 171856 171856	Soft Exp 0 0
Properties of tunnel to: Status Source enabled 192.168.0.1 enabled 192.168.0.2	192.168.0.2 Destination E 192.168.0.2 3 192.168.0.1 3	ncrypti Authentication DES HMAC-SHA1 DES HMAC-SHA1	SPI 01a51041 d9763ae1	Bytes Elapsed 38408 9216	Soft Expira 154576 154576	Hard Expira 171856 171856	Soft Exp 0 0
Properties of tunnel to: Status Source enabled 192.168.0.1 enabled 192.168.0.2	192.168.0.2 Destination E 192.168.0.2 3 192.168.0.1 3	ncrypti Authentication DES HMAC-SHA1 DES HMAC-SHA1	SPI 01a51041 d9763ae1	Bytes Elapsed 38408 9216	Soft Expira 154576 154576	Hard Expira 171856 171856	Soft Exp 0 0
Properties of tunnel to: Status Source enabled 192168.0.1 enabled 192.168.0.2	192.168.0.2 Destination E 192.168.0.2 3 192.168.0.1 3	ncrypti Authentication DES HMAC:SHA1 DES HMAC:SHA1	SPI 01a51041 d9763ae1	Bytes Elapsed 38408 9216	Soft Expira 154576 154576	Hard Expira 171856 171856	Soft Exp 0 0
Properties of tunnel to: Status Source enabled 192.168.0.1 enabled 192.168.0.2	192.168.0.2 Destination E 192.168.0.2 3 192.168.0.1 3	ncrypti Authentication DES HMAC-SHA1 DES HMAC-SHA1	SPI 01a51041 d9763ae1	Bytes Elapsed 38408 9216	Soft Expira 154576 154576	Hard Expira 171856 171856	Soft Exp 0 0
Properties of tunnel to: Status Source enabled 192.168.0.1 enabled 192.168.0.2	192.168.0.2 Destination E 192.168.0.2 3 192.168.0.1 3	ncrypti Authentication DES HMAC-SHA1 DES HMAC-SHA1 IIII	SPI 01a51041 d9763ae1	Bytes Elapsed 38408 9216	Soft Expira 154576 154576	Hard Expira 171856 171856	Soft Exp 0 0
Properties of tunnel to: Status Source enabled 192.168.0.1 enabled 192.168.0.2 Auto Refresh 5	192.168.0.2 Destination E 192.168.0.2 3 192.168.0.1 3 192.168.0.1 3 ■ Seconds	ncrypti Authentication DES HMAC-SHA1 DES HMAC-SHA1	SPI 01a51041 d9763ae1	Bytes Elapsed 38408 9216 Re	Soft Expira 154576 154576	Hard Expira 171856 171856	Soft Exp 0 0
Properties of tunnel to: Status Source enabled 192.168.0.1 enabled 192.168.0.2 Auto Refresh 5	192.168.0.2 Destination E 192.168.0.2 3 192.168.0.1 3 192.168.0.1 3 Seconds	ncrypti Authentication DES HMAC-SHA1 DES HMAC-SHA1 MAC-SHA1	SPI 01a51041 d9763ae1	Bytes Elapsed 38408 9216 Re	Soft Expira 154576 154576	Hard Expira 171856 171856	Soft Exp 0 0
Properties of tunnel to: Status Source enabled 192168.0.1 enabled 192168.0.2 Auto Refresh 5	192.168.0.2 Destination E 192.168.0.2 3 192.168.0.1 3 192.168.0.1 3 Seconds	ncrypti Authentication DES HMAC-SHA1 DES HMAC-SHA1	SPI 01a51041 d9763ae1	Bytes Elapsed 38408 9216 Re	Soft Expira 154576 154576	Hard Expira 171856 171856	Soft Exp 0 0

- Mane	odule1 192	Address	Known By configured	Tunnel Status					
Endpoir	its behind: м	192.168.0.1	Knowin Bu	Known By:	config et ID /Subpet	jured			
19 19	32.168.0.4 00	0:11:25:85:AA:40	learned	Jubr	ector 5 donec	IIIdok			
Properti	es of tunnel to:	192.168	0.1						
	Source	Destination	Encryption	n Authenti	SPI	Bytes Elapsed	Soft Expira	Hard Expira	Soft
Status			20.00	LIMAC	01a51041	43712	154162	171442	0
Status enabled	192.168.0.1	192.168.0.2	3DES SDEC	HMAC	407021	10022	15/102	171442	0
Status enabled enabled	192.168.0.1 192.168.0.2	192.168.0.2 192.168.0.1	3DES 3DES	HMAC	d9763ae1	10022	154162	171442	0

第六章 路由

Copyright © Siemens

6.1 路由概述

路由器的主要作用是连通不同网段的 IP 网络,另外可以选择信息传送的线路。选择通畅快捷 的近路,能大大提高通信速度,减轻网络系统通信负荷,节约网络系统资源,提高网络系统畅通 率,从而让网络系统发挥出更大的效益来。

从过滤网络流量的角度来看,路由器的作用与交换机非常相似。但是与工作在网络第二层的 交换机不同,路由器使用专门的软件协议从逻辑上对整个网络进行划分。例如,一台支持 IP 协议 的路由器可以把网络划分成多个子网段,只有指向特殊 IP 地址的网络流量才可以通过路由器。对 于每一个接收到的数据包,路由器都会重新计算其校验值,并写入新的物理地址。因此,使用路 由器转发和过滤数据的速度往往要比只查看数据包物理地址的交换机慢。但是,对于那些结构复 杂的网络,使用路由器可以提高网络的整体效率。另外,网络中会存在广播数据,而大量的广播 会消耗网络带宽,无谓的占用了网络资源,使网络的传输效率降低。路由器可以自动过滤网络广 播,是路由器的另外一个优点。

从总体上说,在网络中添加路由器的整个安装过程要比即插即用的交换机复杂很多。一般说 来,异构网络互联与多个子网互联都应采用路由器来完成。路由器的主要工作就是为经过路由器 的每个数据帧寻找一条最佳传输路径,并将该数据有效地传送到目的站点。由此可见,选择最佳

路径的策略即路由算法是路由器的关键所在。为了完成;这项工作,在路由器中保存着各种传输 路径的相关数据——路由表(Route Table),供路由选择时使用。

路由表可以是由系统管理员固定设置好的,也可以由系统动态修改。由系统管理员事先设置 好固定的路由表称之为静态(static)路由表,一般是在系统安装时就根据网络的配置情况预先设 定的,它不会随未来网络结构的改变而改变。动态(Dynamic)路由表是路由器根据网络系统的 运行情况而自动调整的路由表。路由器根据路由选择协议(Routing Protocol)提供的功能,自动 学习和记忆网络运行情况,在需要时自动计算数据传输的最佳路径。

SCALANCE S 提供基本的路由功能,需要人为的手动添加来完成。SCALANCE S 由于具有防火 墙功能,需要在路由组态是组态过滤策略,这样才能实现设备之间的相互通讯。

6.2 路由组态



主机 Host2 与 SCALANCE S 端口 1 相连,主机 Host3 与 SCALANCE S 端口 2 相连。Host2 位于子 网 2 中,该网段的 IP 网关为 192.168.10.1/24,Host3 位于子网 3 中,该网段 IP 网关为

192.168.20.1/24。具体 IP 地址参考网络组态图。

号	组态步骤									
	<u> </u>	夕和应	ᇳᇥᆇ	- Doute	5 目体但:		ᇬᄱᅕᅹ	政 大市日	3	人中人世
	│利廷坝日用厂 │	石州密	的均力	ROULE	,异仲纽:	心多考 DHU	P狙心刃	豫。仕坝日	中加入	个女王侠
	块 S612 V2。	根据网	络组态	图设置	륍IP 地址,	子网掩码并	f相应添力	I SCALANC	ES的M	AC 地址。
	<table-of-contents> Security Configura</table-of-contents>	tion Tool [C	onfiguratio	on1 C:Pro	ogram Files\sieme	ns\Security_Config	uration_Tool\Pro	ojects\]*		
	<u>Project Edit Insert Tra</u>	nsfer <u>V</u> iew ⊆	ptions <u>H</u> elp							
			1 🔬 🔉	9 						
	Offline View	Number	Name	Туре	IP Address ext.	Subnet Mask ext.	IP Address int.	Subnet Mask int.	Default Router	MAC Address
	E Carl All Modules Module1	1	Module1	S612 V2	192.168.10.1	255.255.255.0				08-00-06-96-9A-E
	Ready					Current	User: route Role:	Admin	Standard	Mode Offline

📄 Network 🛄 Firewall Settings 🥮 Time Synchronization 📜 Routing Modus
Routing
external module IP address 192.168.10.1 external subnetmask 255.255.255.0
internal module IP address 192.168.20.1 internal subnetmask 255.255.255.0
点击OK 按钮结束,并保存项目。 Security Configuration Tool [route C:\Program Files\SIEMENS\Security_Configuration_Tool\Projects\route\] Project Edt Insert Transfer View Options Help Project Edt Insert Transfer View Insert View Insert View Insert View Insert Type IP Address ext. Submet Mask ext. IP Address int. Submet Mask int. Default Router MAC. Project Project Insert Transfer View Insert View Ins
点击OK 按钮结束,并保存项目。 Security Configuration Tool [route C:\Program Files\SIEMENS\Security_Configuration_Tool\Projects\route\] Project Edit Insert Iransfer View Options Help DIFFERENT



Tunnel communication only	Allow access to NTP server from internal to external network
Allow IP traffic from internal to external network	Allow SiClock time messages from external to internal network
Allow IP traffic with S7 protocol from internal to external network	Allow access to DNS server from internal to external network
Allow access to DHCP server from internal to external network	Allow configuration of nodes via DCP
P Logging	MAC Log Settings
Log tunneled packets	Log passed packets
Log blocked incoming packets	Log blocked incoming packets
Log blocked outgoing packets	Log blocked outgoing packets
nis module is in routing mode. The	refore the MAC rules will not be applied.
	OK Cancel Hel

copyright © Siemens AG Copyright year All rights reserved

		102 2000					2022
Action	Direction	Source IP	Destinatio	n IP	(all)	Bandwidth(M.
Drop	External->Internal				(all)		
	()	1		ř – ř	1		ì
Expand Rulesets	Collapse Rulesets	Add Rule	Remove Rule	t		ervice Definitions	
						1.1	
·PC主机 H nternet Pro General You can get	Host2 设置 IP 和 tocol (TCP/IP) Pr	和网关。 operties automatically if your r	? network supports		<u></u> OK	Cancel	
PC 主机 H nternet Pro General You can get this capabilit the appropria	HOST2 设置 IP 和 tocol (TCP/IP) Pr IP settings assigned a y. Otherwise, you nee ate IP settings.	和网关。 <mark>roperties</mark> automatically if your r ed to ask your networ	network supports k administrator for		<u> </u>	Cancel	
PC 主机 H nternet Pro General You can get this capabilit the appropria	HOST2 设置 IP 和 tocol (TCP/IP) Pr IP settings assigned a y. Otherwise, you nee ate IP settings. an IP address automa	和网关。 <mark>operties</mark> automatically if your r ed to ask your network atically	retwork supports k administrator for		<u></u>	Cancel	
PC 主机 H nternet Pro General You can get this capabilit the appropria ① @btain	HOST2 设置 IP 和 tocol (TCP/IP) Pr IP settings assigned a y. Otherwise, you nee ate IP settings. an IP address automa e following IP address	和网关。 <mark>operties</mark> automatically if your r ed to ask your network atically	network supports k administrator for		<u>DK</u>	Cancel	
PC 主机 H nternet Pro General You can get this capabilit the appropria ① Dbtain ① Use the IP addres	Host2 设置 IP 和 tocol (TCP/IP) Pr IP settings assigned a y. Otherwise, you nee ate IP settings. an IP address automa e following IP address s:	和网关。 operties automatically if your r ed to ask your network atically	retwork supports k administrator for		<u></u>	Cancel	
PC 主机 H nternet Pro General You can get this capabilit the appropria ① <u>D</u> btain ① <u>Q</u> btain ① <u>Q</u> se the <u>I</u> P addres S <u>u</u> bnet m	Host2 设置 IP 和 tocol (TCP/IP) Pr IP settings assigned a y. Otherwise, you nee ate IP settings. an IP address automa a following IP address s: ask:	和网关。 operties automatically if your r d to ask your network atically 192.168. 255.255.3	retwork supports k administrator for 10 . 4 255 . 0		<u>DK</u>	Cancel	
PC 主机 H nternet Pro General You can get this capabilit the appropria ① Dotain ① Use the IP addres Sybnet m Default or	HOST2 设置 IP 和 tocol (TCP/IP) Pr IP settings assigned a y. Otherwise, you nee ate IP settings. an IP address automa a following IP address s: ask: ask:	和网关。 operties automatically if your r rd to ask your network atically 192.168. 255.255.1 192.168.	retwork supports k administrator for		DK	Cancel	
PC 主机 H Internet Pro General You can get this capabilit the appropria ① Detain ① Detain IP addres Subnet m Default ga	Host2 设置 IP 和 tocol (TCP/IP) Pr IP settings assigned a y. Otherwise, you nee ate IP settings. an IP address automa a following IP address s: ask: ateway:	和网关。 operties automatically if your r d to ask your network atically 192.168. 255.255.3 192.168.	retwork supports k administrator for 10 . 4 255 . 0 10 . 1		<u> </u>	Cancel	
PC 主机 H Internet Pro General You can get this capabilit the appropria ① Dotain ① Use the IP addres Subnet m Default ga O Dotain	HOST2 设置 IP 和 tocol (TCP/IP) Pr IP settings assigned a y. Otherwise, you nee ate IP settings. an IP address automa e following IP address s: ask: asteway: DNS server address a	和网关。 operties automatically if your red to ask your network atically 192.168. 192.168. 192.168.	retwork supports k administrator for 10 . 4 255 . 0 10 . 1		DK	Cancel	
PC 主机 H Internet Pro General You can get this capabilit the appropria ① Dotain ② Use the Subnet m Default ge ③ Obtain ③ Use the	HOST2 设置 IP 和 tocol (TCP/IP) Pr IP settings assigned a y. Otherwise, you nee ate IP settings. an IP address automa e following IP address s: ask: ateway: DNS server address a e following DNS serve	和网关。 operties automatically if your r ed to ask your network atically 192 . 168 . 255 . 255 . : 192 . 168 . automatically er addresses:	retwork supports k administrator for 10 4 255 0 10 1		DK	Cancel	
PC 主机 H Internet Pro General You can get this capabilit the appropria ① Detain ① Use the Default ga ② Use the Preferred	HOST2 设置 IP 和 tocol (TCP/IP) Pr IP settings assigned a y. Otherwise, you nee ate IP settings. an IP address automa a following IP address s: ask: ateway: DNS server address a following DNS serve DNS server:	和网关。 operties automatically if your r ed to ask your network atically 192 . 168 . 255 . 255 . : 192 . 168 . automatically er addresses:	10 4 255 0 10 1		DK	Cancel	
PC 主机 H nternet Pro General You can get this capabilit the appropria ① Use the IP addres Subnet m Default ga ① Use the Preferred Alternate	HOST2 设置 IP 和 tocol (TCP/IP) Pr IP settings assigned a y. Otherwise, you nee ate IP settings. an IP address automa a following IP address s: ask: asteway: DNS server address a e following DNS serve DNS server: DNS server:	和网关。 operties automatically if your r ed to ask your network atically 192 . 168 . 255 . 255 . : 192 . 168 . automatically er addresses:	etwork supports administrator for		<u>DK</u>	Cancel	
PC 主机 H nternet Pro General You can get this capabilit the appropria ① ①btain ① ①se the ① ② Use the ① ①btain ③ ①se the ② ①se the Preferred △ lternate	HOST2 设置 IP 和 tocol (TCP/IP) Pr IP settings assigned 4 y. Otherwise, you nee ate IP settings. an IP address automa e following IP address s: ask: ateway: DNS server address a e following DNS serve DNS server: DNS server:	和网关。 operties automatically if your r d to ask your network atically 192 . 168 . 255 . 255 . ; 192 . 168 . automatically er addresses:	retwork supports k administrator for 10 . 4 255 . 0 10 . 1		DK	Cancel	
PC 主机 H nternet Pro General You can get this capabilit the appropria ① Datain ① Use the Default ga ② Use the Default ga ② Use the Preferred Alternate	Host2 设置 IP 和 tocol (TCP/IP) Pr IP settings assigned a y. Otherwise, you nee ate IP settings. an IP address automa a following IP address s: ask: asteway: DNS server address a e following DNS serve DNS server: DNS server:	和网关。 operties automatically if your r d to ask your network atically 192.168. 192.168. 192.168. automatically er addresses: 	Petwork supports k administrator for 10 . 4 255 . 0 10 . 1		<u>DK</u>	Cancel	
PC 主机 H nternet Pro General You can get this capabilit the appropria ① <u>D</u> btain ① <u>D</u> btain ① <u>U</u> se the <u>D</u> efault get ② <u>U</u> se the <u>P</u> referred <u>A</u> lternate	HOST2 设置 IP 和 tocol (TCP/IP) Pr IP settings assigned a y. Otherwise, you nee ate IP settings. an IP address automa a following IP address s: ask: ateway: DNS server address a following DNS serve DNS server: DNS server:	和网关。 operties automatically if your r ed to ask your network atically 192 . 168 . 255 . 255 . : 192 . 168 . automatically er addresses:	retwork supports k administrator for		DK	Cancel	

	Internet Protocol (TCP/IP) Pr	operties	3	
	General			
	You can get IP settings assigned a this capability. Otherwise, you nee the appropriate IP settings.	automatically if your network supports d to ask your network administrator for		
	O <u>O</u> btain an IP address automa	itically		
	Ose the following IP address:	·		
	IP address:	192.168.20.5		
	S <u>u</u> bnet mask:	255 . 255 . 255 . 0		
	Default gateway:	192.168.20.1		
	O <u>D</u> tain DNS server address a	sutomatically		
	• Use the following DNS serve	r addresses:		
	Preferred DNS server:			
	Alternate DNS server:			
		Ad <u>v</u> anced		
	·	OK Cancel		
5	使用 Ping 功能测试路由功	能。Host2 使用 Ping 到 Host3	3。测试结果不通。	
	C:\WINDOWS\system32\	CMD exe		1
			· · · · · · · · · · · · · · · · · · ·	
	C:\Documents and Setti	ngs>ping 192.168.20.5		1
	Pinging 192.168.20.5 w	ith 32 bytes of data:		
	Request timed out			
	Request timed out.			1
	Request timed out. Request timed out.			
		0-1/0-00 5-		
	Packets: Sent = 4,	Received = 0, Lost = 4 (1	100% loss),	
	C:\Documents and Setti	nas>		
				1
	Host3 使用 Ping 到 Host2。	测试结果通。实现内网到外	网的路由功能。	
	5			

	C:\WINDOWS\System32\cmd.exe	- 🗆 🗙
	C:\Documents and Settings\Administrator>ping 192.168.10.4	
	Pinging 192.168.10.4 with 32 bytes of data:	
	Reply from 192.168.10.4: bytes=32 time<1ms TTL=127 Reply from 192.168.10.4: bytes=32 time<1ms TTL=127 Reply from 192.168.10.4: bytes=32 time<1ms TTL=127 Reply from 192.168.10.4: bytes=32 time<1ms TTL=127	
	Ping statistics for 192.168.10.4: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = Oms, Maximum = Oms, Average = Oms	•
6	点击工具栏按钮 🚰,双击右侧栏的 Module1 图标。可以查看 module1 的包过滤日志信	息。点
	击 Start reading 按钮,弹出 Log Settings 对话框,点选 IP、Dropped Packets 和 Passed F	Packets
	3个选项。	
	Log Settings X Categories Capture	
	IP (Layer 3)	
	MAC (Layer 2)	
	Compared Packets	
	Passed Packets	
	OK Cancel	
	观察包的过滤信息。	

No.	Date	Time	Source	Destination	Protocol	Interface	Action	Direction
* 176	2/14/2008	1:24:58 PM.84	192.168.20.05	192.168.10.04	Icmp	Ext	Passed	Out
2 177	2/14/2008	1:24:58 PM.84	192.168.10.04	192.168.20.05	Icmp	Ext	Passed	In
* 178	2/14/2008	1:24:59 PM.84	192.168.20.05	192.168.10.04	lomp	Ext	Passed	Out
2 179	2/14/2008	1:24:59 PM.84	192.168.10.04	192.168.20.05	Icmp	Ext	Passed	In
180	2/14/2008	1:25:00 PM.77	192,168,10,04	192.168.20.06	lcmp	Ext	Dropped	In
* 181	2/14/2008	1:25:00 PM.84	192.168.20.05	192.168.10.04	Icmp	Ext	Passed	Out
* 182	2/14/2008	1:25:00 PM.84	192.168.10.04	192.168.20.05	Icmp	Ext	Passed	In
* 183	2/14/2008	1:25:01 PM.85	192.168.20.05	192.168.10.04	Icmp	Ext	Passed	Out
* 184	2/14/2008	1:25:01 PM.85	192.168.10.04	192.168.20.05	lomp	Ext	Passed	In
* 185	2/14/2008	1:25:02 PM.85	192.168.20.05	192.168.10.04	lemp	Ext	Passed	Out
* 186	2/14/2008	1:25:02 PM.85	192.168.10.04	192.168.20.05	Icmp	Ext	Passed	In
* 187	2/14/2008	1:25:03 PM.85	192.168.20.05	192.168.10.04	Icmp	Ext	Passed	Out
* 188	2/14/2008	1:25:03 PM.85	192.168.10.04	192.168.20.05	lemp	Ext	Passed	In
* 189	2/14/2008	1:25:04 PM.85	192.168.20.05	192.168.10.04	lcmp	Ext	Passed	Out
* 190	2/14/2008	1:25:04 PM.85	192.168.10.04	192.168.20.05	lemp	Ext	Passed	In
* 191	2/14/2008	1:25:05 PM.85	192.168.20.05	192.168.10.04	lemp	Ext	Passed	Out
* 192	2/14/2008	1:25:05 PM.85	192.168.10.04	192.168.20.05	Icmp	Ext	Passed	In
* 193	2/14/2008	1:25:06 PM.85	192.168.20.05	192.168.10.04	lomp	Ext	Passed	Out
* 194	2/14/2008	1:25:06 PM.85	192.168.10.04	192.168.20.05	Icmp	Ext	Passed	In
<					(

第七章 NAT/NAPT

Copyright © Siemens AG Copyright year All rights reserved

7.1 NAT/NAPT 概述

随着 Internet 的迅速发展, IP 地址短缺已成为一个十分突出的问题。已经有很多种方法 来减轻 IP 地址扩展问题的方案。比如,使用私有地址(在 RFC1918 中定义),变长子网掩码 (VLSM, Variable-length subnet mask),无类域间路由(CIDR, Classless inter-domain routing),地址转换(NAT 和 PAT),动态地址池(如 DHCP)及 IPv6。但最根本的解决 IP 地址不 足的问题的方法还是尽快实现 IPv6。

为了减少公有 IP 地址的浪费,一种解决方法是在广域网链路上使用私有地址。但是,在 广域网链路上使用私有地址的一个条件就是在这些链路上使用的私有地址不能是去往因特网 的通信的起始源,或是来自因特网的通信的最终目的。为满期足这一条件 NAT 技术应运而生。

NAT (Network Address Translation)的功能,就是指在一个网络内部,根据需要可以随意 自定义 IP 地址,而不需要经过申请。在网络内部,各计算机间通过内部的 IP 地址进行通讯, 而当内部的计算机要与外部 Internet 网络进行通讯时,具有 NAT 功能的设备(比如路由器)负 责将其内部的 IP 地址替换(Translation)为合法的 IP 地址(即经过申请的 IP 地址)进行通信。 NAPT (Network Address Port Transition) 的功能是与 NAT 的概念是相当接近的,也就是端口地址解析。与 NAT 技术的不同,数据是内部网络主机的 IP 地址和端口号在通过路由器时被替换修改为(Translation)外部网络的 IP 地址和端口号。

SCALANCE S 支持 NAT 和 NAPT 功能,这样可以对于 SCALANCE S 所连接的内网设备进行保护 (内部网络)。另外,对于很多重复的网络且其内部带有相同 IP 的设备,使用 NAT 的方法进行 访问是非常有效的。另外,由于 SCALANCE S 同时又具有防火墙功能,这样在实现了 NAT/NAPT 后,数据才会经过防火墙,所以需要在路由组态后,组态正确的过滤策略,这样才能实现设备之 间的相互通讯。



主机 Host2 与 SCALANCE S 端口 1 相连,主机 Host3 与交换机 SCALANCE X400 相连,交换机 SCALANCE X400 与 SCALANCE S 的端口 2 相连。Host2 位于外网 2 中,该网段的 IP 网关为 192.168.10.1/24, SCALANCE X-400 和 Host3 位于内网中,该网段 IP 网关为 192.168.20.1/24。 具体 IP 地址参考网络组态图。

序号	组态步骤
1	新建项目用户名和密码均为 NAT,具体参考路由组态到步骤 3。点击 View 菜单,选择
	Advanced mode。双击右侧栏 Module1 的图标,弹出高级模式的模块属性对话框。选择
	Routing Modus 栏。使能 NAT active 和 Allow Internal->External for all users。这样所有内部设
	备可以给外部网络设备发送通讯请求。使能 NAPT active,给内网的设备 SCALANCE X-400 设置
	外部端口号 15000。注意需要配置在 8000 和 65535 之间的端口号。

pyright © Siemens	G Copyright year	vII rights reserved
Cop	ВA В	Ā

	rk trewall	Settings	SSL Certificate	🕒 Time Synchron	ization 💭 Logg	ing 🛃
	Se VPN	L	동력, Houting Modu	s]	🗳 DH	CP-Server
Routing						
Routi	ng active					
external	module IP address 19	92.168.10.1	external subnetmask	255.255.255	5.0	
internal r	nodule IP address 15	32.168.20.1	internal subnetmask	255.255.255	5.U	
NAT				NAPT		
✓ NAT	active			✓ NAPT active		
Allow	Internal->External for all	users		external IP addre	ss 192,168,10,1	
extern	al IP address 🛛 interna	al IP address 🛛 🛛	Direction	external port	internal IP address	internal port
				15000	192.168.20.6	80
			1.40			
192.168	.10.1 *	In	ternal->External			
		1.12	1	,		1
	Add	Remove	•		Add F	Remove
					OK Ca	incel H
∙1± LOG 1:	兰激活日志功能	₺。保存项	目并下载。			
odule Propert	兰激活日志功能 ties - Module1 W Firewall Settings 国	E。保存项目 SSL Certificate)	目并下载。 © Time Synchronization §	년 Logging 문희 Node	es 🕯 VPN 📒 Routin	g Modus 🛃 DF
odule Propert	兰激活日志功能 ties - Module1 IIII Firewall Settings ाञ MAC Rules (inactive)	E。保存项目 SSL Certificate €	目并下载。 ◎ Time Synchronization §	원 Logging 🛃 Node	es 🐋 VPN 💺 Routin	g Modus 🕰 DH
1± LOG 1: odule Propert Network Network Network IP Rules N Action Allow	兰激活日志功能 ties - Module1 描 Firewall Settings MAC Rules (inactive) Direction Internal->External	E。保存项目 SSL Certificate ↓ ↓ Source IP	目并下载。 © Time Synchronization & Destination	김 Logging 勇 Node P Servi (all)	es 😒 VPN 🛃 Routin ce Bandw	g Modus 🖉 DH ridth(M Log vi
Action Allow Allow	兰激活日志功能 t <mark>ies - Module 1</mark> 때 Firewall Settings [☑ MAC Rules (inactive) 〕Direction Internal->External External->Internal	E。保存项目 SSL Certificate ↓ Source IP	目并下载。 Time Synchronization & Destination 1 192.168.20.	Degging Definition Node P Servi 6 (all)	es 🐋 VPN 🛃 Routin ce Bandw	g Modus 🕰 DH idth(M Log 식 식
Attion	兰激活日志功能 ties - Module1 描 Firewall Settings AC Rules (inactive) Direction Internal->External External->Internal	E。保存项目 SSL Certificate ∉ ↓ Source IP	目并下载。 ◎ Time Synchronization &	Degging B Node P Servi (all) 6 (all)	es 🐋 VPN 💼 Routin ce Bandw	g Modus 🕑 DH idth(M Log 식
Action Allow Allow	兰激活日志功能 t <mark>ies - Module1</mark> 描 Firewall Settings MAC Rules (inactive) Direction Internal->External External->Internal	E。保存项目 SSL Certificate SSL Certificate Source IP	■并下载。 Time Synchronization Destination 192.168.20.1	Degging B Node P Servi (all) 6 (all)	es 😒 VPN 🛃 Routin ce Bandw	g Modus 🕰 DH idth(M Log 식 식
Action Allow	兰激活日志功能 T <mark>tes - Module1</mark> III Firewall Settings [□] MAC Rules (inactive) Direction Internal->External External->Internal	E。保存项目 SSL Certificate ↓ Source IP	■并下载。 Time Synchronization Destination 1 192.168.20.1	D Logging 📃 Node P Servi (all) 6 (all)	es 🐋 VPN 💼 Routin ce Bandw	g Modus 🛃 DH idth(M Log
Action Allow	兰激活日志功能 ties - Module1 描 Firewall Settings MAC Rules (inactive) Direction Internal->External External->Internal	E。保存项目 SSL Certificate SSL Certificate Source IP	目并下载。 ◎ Time Synchronization &	Logging 🔁 Node P Servi (all) 6 (all)	es 🐋 VPN 🛃 Routin ce Bandw	g Modus 🛃 DH idth(M Log
Action Allow	兰激活日志功能 tes - Module1 描 Firewall Settings □ AC Rules (inactive) Direction Internal->External External->Internal	E。保存项目 SSL Certificate ↓ Source IP	目并下载。 ◎ Time Synchronization ◎ Destination 192.168.20.	Logging 💭 Nod P Servi 6 (all)	es 🐋 VPN 🛃 Routin ce Bandw	g Modus 🕰 DH idth(M Log 식 식
Action Allow Allow	兰激活日志功能 Tes - Module1 描 Firewall Settings □ AAC Rules (inactive) Direction Internal->External External->Internal	E。保存项目 SSL Certificate ↓ Source IP	目并下载。 ◎ Time Synchronization &	Degging Book	es 🐋 VPN 🖶 Routin ce Bandw	g Modus 🛃 DH idth(M Log
Action Allow Allow	兰激活日志功能 ites - Module1 描 Firewall Settings ☑ ACC Rules (inactive) Direction Internal->External External->Internal	E。保存项目 SSL Certificate SSL Certificate Source IP	目并下载。 ◎ Time Synchronization &	Logging 📜 Node P Servi (all) 6 (all)	es 📽 VPN 🖶 Routin ce Bandw	g Modus 🛃 DH idth(M Log
Action Allow Allow	兰激活日志功能 Tes - Module 1 描 Firewall Settings □ AC Rules (inactive) Direction Internal->External External->Internal	E。保存项目 SSL Certificate ↓ Source IP	■ 并下载。 Time Synchronization Destination 1 192.168.20.1	Logging Servi P Servi (all)	es 🛸 VPN 🔁 Routin	g Modus 🕰 DH idth(M Log 1 1
Action Allow Allow	兰激活日志功能 tres - Module1 描 Firewall Settings □ AAC Rules (inactive) Direction Internal->External External->Internal	E。保存项目 SSL Certificate €	目并下载。 ■ Time Synchronization & Destination I 192.168.20.1	Logging B Node P Servi (all) 6 (all)	es 🐋 VPN 🔁 Routin	g Modus 또 DH idth(M Log
Action Allow Allow	兰激活日志功能 ties - Module1 描 Firewall Settings ☑ ACC Rules (inactive) Direction Internal->External External->Internal	E。保存项目 SSL Certificate	■并下载。 Time Synchronization Destination I 192.168.20.1	Logging B Node P Servi (all) 6 (all)	es 🕬 VPN 🔁 Routin	g Modus DF
Action Allow Allow Expand Rulesets	兰激活日志功能 Tes - Module 1 描 Firewall Settings □ AC Rules (inactive) Direction Internal->External External->Internal External->Internal Collapse Rulesets	E。保存项目 SSL Certificate	■ 并下载。 Time Synchronization Destination 192.168.20.1	Logging Dervi P Servi (all) 6 (all) 1 1 1 1 1 1 1 1 1 1 1 1 1	es WPN 💼 Routin	g Modus S DF
Action Allow Allow Expand Rulesets	兰激活日志功能 Harmonia Contraction (1998) External->Internal (1998) E	E。保存项目 SSL Certificate	■ 并下载。 Time Synchronization ほ Destination I 192.168.20.1	Logging B Node P Servi (all) 6 (all) 5	es 📽 VPN 🛃 Routin ce Bandw IP Service Definitions	g Modus 🖉 DF
Action Allow Allow Expand Rulesets	兰激活日志功能 Tes - Module 1 描 Firewall Settings □ AAC Rules (inactive) Direction Internal->External External->Internal External->Internal Collapse Rulesets	E。保存项目 SSL Certificate	■ 并下载。 Time Synchronization Destination I 192.168.20.1	Logging S Node P Servi (all) 6 (all) 7	es WPN B Routin	g Modus 🛃 D+ idth(M Log 4 4
Action Allow Allow Expand Rulesets	兰激活日志功能 thes - Module1 描 Firewall Settings □ AAC Rules (inactive) Internal->External External->Internal External->Internal Collapse Rulesets	E。保存项目 SSL Certificate 4 Source IP	■ 并下载。 Time Synchronization Destination 1 192.168.20.1	Logging E Node P Servi (all) 6 (all) 1 1 1 1 1 1 1 1 1 1 1 1 1	es S VPN B Routin	g Modus 🖉 Dł idth (M Log 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Action Allow Allow Allow Allow Allow	兰激活日志功能 Tes - Module 1 描 Firewall Settings □ AC Rules (inactive) Direction Internal->External External->Internal External->Internal Collapse Rulesets	E。保存项目 SSL Certificate	■ 并下载。 Time Synchronization Destination 1 192.168.20.1	Logging B Node P Servi (all) 6 (all) 1 1 1 1 1 1 1 1 1 1 1 1 1	es VPN B Routin	g Modus

pyright © Siemens	G Copyright year	II rights reserved
Copy	AG	P

aeneral		
You can get IP settings assigne this capability. Otherwise, you ne the appropriate IP settings.	d automatically if your network supports sed to ask your network administrator for	
O Dbtain an IP address autor	natically	
Ose the following IP address		
IP address:	192.168.10.4	
S <u>u</u> bnet mask:	255 . 255 . 255 . 0	
Default gateway:	192.168.10.1	
O 0btain DNS server address	: automatically	
• Use the following DNS ser	ver addresses:	
Preferred DNS server:		
Alternate DNS server:		
	âdvanced	
	OK Cancel	
PC 主机 Host3 设置 IP ternet Protocol (TCP/IP)	和网关。	ก
PC 主机 Host3 设置 IP nternet Protocol (TCP/IP) I General	和网关。 Properties	
PC 主机 Host3 设置 IP nternet Protocol (TCP/IP) General You can get IP settings assigne this capability. Otherwise, you n the appropriate IP settings.	和网关。 Properties @ Comparison Com	
PC 主机 Host3 设置 IP Iternet Protocol (TCP/IP) General You can get IP settings assigne this capability. Otherwise, you n the appropriate IP settings.	和网关。 Properties ? d automatically if your network supports eed to ask your network administrator for matically	
PC 主机 Host3 设置 IP nternet Protocol (TCP/IP) General You can get IP settings assigne this capability. Otherwise, you n the appropriate IP settings. ① <u>D</u> btain an IP address auto ④ Use the following IP address	和网关。 Properties @ () () () () () () () () () () () () ()	
PC 主机 Host3 设置 IP Iternet Protocol (TCP/IP) General You can get IP settings assigne this capability. Otherwise, you n the appropriate IP settings. ① @btain an IP address auto ④ Uge the following IP addres _IP address:	和网关。 Properties @ comparison @	
PC 主机 Host3 设置 IP nternet Protocol (TCP/IP) General You can get IP settings assigne this capability. Otherwise, you n the appropriate IP settings. ① @btain an IP address auto ④ Use the following IP addres IP address: Sybnet mask:	和网关。 Properties @ () () () () () () () () () () () () ()	
PC 主机 Host3 设置 IP Iternet Protocol (TCP/IP) General You can get IP settings assigne this capability. Otherwise, you n the appropriate IP settings. ① @btain an IP address auto ③ Use the following IP addres IP address: Subnet mask: Default gateway:	和网关。 Properties ? d automatically if your network supports eed to ask your network administrator for matically ss: 192.168.20.5 255.255.255.0 192.168.20.1	
PC 主机 Host3 设置 IP Iternet Protocol (TCP/IP) General You can get IP settings assigne this capability. Otherwise, you n the appropriate IP settings. ① @btain an IP address auto ③ @btain an IP address auto ④ Use the following IP addres IP address: Subnet mask: Default gateway: ④ @btain DNS server address	和网关。 Properties ? d automatically if your network supports eed to ask your network administrator for matically ss: 192.168.20.5 255.255.255.0 192.168.20.1	
PC 主机 Host3 设置 IP Internet Protocol (TCP/IP) (General You can get IP settings assigned this capability. Otherwise, you ne the appropriate IP settings. ① Dbtain an IP address auto ④ Use the following IP addres IP address: Sybnet mask: Default gateway: ④ Obtain DNS server address ④ Use the following DNS server address ④ Use the following DNS server address	和网关。 Properties Prope	
PC 主机 Host3 设置 IP Iternet Protocol (TCP/IP) General You can get IP settings assigne this capability. Otherwise, you n the appropriate IP settings. ① @btain an IP address auto ④ Uge the following IP addres IP address: Sybnet mask: @efault gateway: ④ @btain DNS server address ④ Use the following DNS server @ Use the following DNS server:	和网关。 Properties Properties Prop	
PC 主机 Host3 设置 IP Iternet Protocol (TCP/IP) General You can get IP settings assigne this capability. Otherwise, you n the appropriate IP settings. ① ①btain an IP address auto ② ①btain an IP address auto ③ ①btain an IP address auto ③ ①btain an IP address auto ④ ①get the following IP addres IP address: Sybnet mask: ① @btain DNS server address ④ Use the following DNS server: ④ Use the following DNS server: ▲Iternate DNS server:	和网关。 Properties Prope	
PC 主机 Host3 设置 IP Iternet Protocol (TCP/IP) General You can get IP settings assigne this capability. Otherwise, you n the appropriate IP settings. ① @btain an IP address auto ④ Uge the following IP addres IP address: Subnet mask: @efault gateway: ④ @btain DNS server address ④ Use the following DNS set Preferred DNS server: Alternate DNS server:	和网关。 Properties Prope	
PC 主机 Host3 设置 IP Iternet Protocol (TCP/IP) General You can get IP settings assigne this capability. Otherwise, you n the appropriate IP settings. ① @btain an IP address auto ④ Uge the following IP addres IP address: Sybnet mask: @efault gateway: ③ @btain DNS server address ④ Usg the following DNS ser Preferred DNS server: Alternate DNS server:	和网关。 Properties Prope	



7	5	测试 NAPT 功能,打开 IE 浏览器,在地址栏内输入//192	. <u>168.10.1:15000</u> 。回车。
reserved		SCALANCE X-400 WEB Management - Microsoft Internet Explorer	
Il rights		File Edit View Favorites Tools Help	💄 🗑 • 🥅 🎇
×		Address 🗃 http://192.168.10.1:15000/	
		SIEMENS	Automation & Drives
		Console Support	SIMATIC NET
		Authorization	
		User name: admin	×
		Password:	
		Logon using a secure HTTPS co	nnection
	6		
	0	点击工具栏按钮 💷,双击右侧栏的 Module1 图标。可J	以查看 module1 的包过滤日志信息。点
		击 Start reading 按钮,弹出 Log Settings 对话框,点选 I	P、Dropped Packets 和 Passed Packets
		3个选项。	
		Log Settings	
		Categories Capture	
		I♥ IP (Layer 3)	
		MAC (Layer 2)	
		✓ Dropped Packets	
		✓ Passed Packets	
		OK Cancel	

Copyright © Siemens AG Copyright year

观察包的过滤信息。

36

2008 1:08:59 PM 2008 1:09:00 PM 2008 1:09:00 PM 2008 1:09:01 PM 2008 1:09:01 PM	I 192.168.10.04 I 192.168.10.01 I 192.168.10.04	192.168.20.05 192.168.10.04 192.168.20.05	lemp lemp	Ext Ext	Passed	In	ICMP: T
2008 1:09:00 PN 2008 1:09:00 PN 2008 1:09:01 PN	I 192.168.10.01 I 192.168.10.04	192.168.10.04 192.168.20.05	lcmp	Ext	D 1		
2008 1:09:00 PN 2008 1:09:01 PN	l 192.168.10.04	192 168 20 05		E 115	Passed	Out	ICMP: T
2008 1:09:01 PM		102.100.20.00	Icmp	Ext	Passed	In	ICMP: T
	I 192.168.10.01	192.168.10.04	Icmp	Ext	Passed	Out	ICMP: T
2008 1:09:01 PM	I 192.168.10.04	192.168.20.05	Icmp	Ext	Passed	In	ICMP: T
2008 1:09:02 PM	I 192.168.10.01	192.168.10.04	Icmp	Ext	Passed	Out	ICMP: 1
2008 1:09:02 PN	I 192.168.10.04	192.168.20.05	lomp	Ext	Passed	In	ICMP: 1
2008 1:09:03 PM	I 192.168.10.01	192.168.10.04	lomp	Ext	Passed	Out	ICMP: 1
2008 1:09:03 PM	I 192.168.10.04	192.168.20.05	Icmp	Ext	Passed	In	ICMP: 1
2008 1:09:04 PM	I 192.168.10.01	192.168.10.04	Icmp	Ext	Passed	Out	ICMP: 1
2008 1:09:04 PM	l 192.168.10.04	192.168.20.05	Icmp	Ext	Passed	In	ICMP: 1
2008 1:09:05 PM	l 192.168.10.01	192.168.10.04	Icmp	Ext	Passed	Out	ICMP: 1
2008 1:09:05 PN	I 192.168.10.04	192.168.20.05	Icmp	Ext	Passed	In	ICMP: 1
	2008 1:09:02 PM 2008 1:09:02 PM 2008 1:09:03 PM 2008 1:09:03 PM 2008 1:09:03 PM 2008 1:09:04 PM 2008 1:09:04 PM 2008 1:09:05 PM 2008 1:09:05 PM 2008 1:09:05 PM	2008 1:09:02 PM 192.168.10.01 2008 1:09:02 PM 192.168.10.04 2008 1:09:03 PM 192.168.10.01 2008 1:09:03 PM 192.168.10.01 2008 1:09:03 PM 192.168.10.01 2008 1:09:04 PM 192.168.10.01 2008 1:09:04 PM 192.168.10.01 2008 1:09:04 PM 192.168.10.01 2008 1:09:05 PM 192.168.10.01 2008 1:09:05 PM 192.168.10.01	2008 1:09:02 PM 192.168.10.01 192.168.10.04 2008 1:09:02 PM 192.168.10.04 192.168.20.05 2008 1:09:03 PM 192.168.10.04 192.168.20.05 2008 1:09:03 PM 192.168.10.04 192.168.20.05 2008 1:09:03 PM 192.168.10.04 192.168.20.05 2008 1:09:04 PM 192.168.10.01 192.168.10.04 2008 1:09:04 PM 192.168.10.04 192.168.20.05 2008 1:09:05 PM 192.168.10.04 192.168.20.05	2008 1:09:02 PM 192.168.10.01 192.168.10.04 Icmp 2008 1:09:02 PM 192.168.10.04 192.168.20.05 Icmp 2008 1:09:03 PM 192.168.10.04 192.168.20.05 Icmp 2008 1:09:03 PM 192.168.10.04 192.168.20.05 Icmp 2008 1:09:03 PM 192.168.10.01 192.168.20.05 Icmp 2008 1:09:04 PM 192.168.10.01 192.168.10.04 Icmp 2008 1:09:04 PM 192.168.10.04 192.168.20.05 Icmp 2008 1:09:05 PM 192.168.10.04 192.168.20.05 Icmp 2008 1:09:05 PM 192.168.10.01 192.168.20.05 Icmp 2008 1:09:05 PM 192.168.10.04 Icmp Icmp 2008 1:09:05 PM 192.168.10.04 192.168.20.05 Icmp	2008 1:09:02 PM 192.168.10.01 192.168.10.04 Icmp Ext 2008 1:09:02 PM 192.168.10.04 192.168.20.05 Icmp Ext 2008 1:09:02 PM 192.168.10.01 192.168.20.05 Icmp Ext 2008 1:09:03 PM 192.168.10.01 192.168.20.05 Icmp Ext 2008 1:09:03 PM 192.168.10.01 192.168.20.05 Icmp Ext 2008 1:09:04 PM 192.168.10.01 192.168.20.05 Icmp Ext 2008 1:09:04 PM 192.168.10.04 192.168.20.05 Icmp Ext 2008 1:09:04 PM 192.168.10.04 192.168.20.05 Icmp Ext 2008 1:09:05 PM 192.168.10.04 192.168.20.05 Icmp Ext 2008 1:09:05 PM 192.168.10.04 192.168.20.05 Icmp Ext 2008 1:09:05 PM 192.168.10.04 192.168.20.05 Icmp Ext	2008 1:09:02 PM 192.168.10.01 192.168.10.04 Icmp Ext Passed 2008 1:09:02 PM 192.168.10.04 192.168.20.05 Icmp Ext Passed 2008 1:09:02 PM 192.168.10.04 192.168.20.05 Icmp Ext Passed 2008 1:09:03 PM 192.168.10.01 192.168.20.05 Icmp Ext Passed 2008 1:09:03 PM 192.168.10.01 192.168.00.5 Icmp Ext Passed 2008 1:09:04 PM 192.168.10.01 192.168.10.04 Icmp Ext Passed 2008 1:09:04 PM 192.168.10.04 192.168.20.05 Icmp Ext Passed 2008 1:09:04 PM 192.168.10.04 192.168.20.05 Icmp Ext Passed 2008 1:09:05 PM 192.168.10.01 192.168.20.05 Icmp Ext Passed 2008 1:09:05 PM 192.168.10.04 192.168.20.05 Icmp Ext Passed 2008	2008 1:09:02 PM 192.168.10.01 192.168.10.04 Icmp Ext Passed Out 2008 1:09:02 PM 192.168.10.04 192.168.20.05 Icmp Ext Passed In 2008 1:09:03 PM 192.168.10.01 192.168.10.04 Icmp Ext Passed In 2008 1:09:03 PM 192.168.10.01 192.168.20.05 Icmp Ext Passed In 2008 1:09:03 PM 192.168.10.01 192.168.20.05 Icmp Ext Passed In 2008 1:09:04 PM 192.168.10.01 192.168.10.04 Icmp Ext Passed Out 2008 1:09:04 PM 192.168.10.01 192.168.20.05 Icmp Ext Passed In 2008 1:09:04 PM 192.168.10.01 192.168.20.05 Icmp Ext Passed Out 2008 1:09:05 PM 192.168.10.01 192.168.20.05 Icmp Ext Passed Out 2008 1:09:05