



# HTTP 正向代理配置手册

网测科技

2021-01-20





1.	文档说明
2.	网络拓扑图
3.	设置防火墙
	3.1 设置接口 ip 地址
	3.2 开启代理
	3.3 添加附加 ip 地址6
	3.4 网络代理的设置
	3.5 添加策略
4.	设置 Supernova 测试仪 12
	4.1 HTTP 的正向代理实例 12
	4.2 启动实例
	4.4 启动后正常运行界面14



## 1. 文档说明

本文档介绍配置 HTTP 正向代理的配置过程,但 HTTP 正向代理的配置涉及 到 HTTP 协议的专业知识、Web 应用的研发逻辑、正则表达式的应用,而且随着 Web 服务器的版本升级和接口变化,需要不断对配置用例进行修改和升级,所以 有任何问题,请联系我们的售前或售后支持人员。

## 2. 网络拓扑图





## 3. 设置防火墙

## 3.1 设置接口 ip 地址

<b>KFV</b>	N	监控▼	系统管理▼	路由▼	防火墙▼	病毒与攻击,	• 上网行为管理 •
系统管理/	网络 /	接口	控制面板	-			
0创建	✔编辑	自删除	网络		接口		
	ו		DHCP服务器		× ×		IP/子网掩码
	]	m1/1	配置	•	选项	2	2 <mark>1.1.1.1 /</mark> 255.255.0.0
	1	<b>m1/2</b> (50C-po	管理员设置	•	DNS 服务器		17.1.1.1 / 255.255.0.0
	1	m1/3	证书	•	网络代理	2	17. <mark>1</mark> .1.1 / 255.255.0.0
	]	<b>m1/4</b> (50C-po	维护			3	18.1.1.1 / 255.255.0.0
	]	port1		_		192.1	68.16.230 / 255.255.255
	1	port2				10.5	8.100.99 / 255.255.255.
	]	port3 (40C_port	:1)			2	27.1.1.1 / 255.255.0.0
	]	port4				2	29.1.1.1 / 255.255.0.0
<b>1</b> 2	1						1111/25525500

#### 我这里用的是 m1/2 和 m1/4 端口

Ø 创建 / 编辑	目 自删除	
	名称	IP/子网掩码
	m1/1	21.1.1.1 / 255.255.0.0
	m1/2 (50C-port1)	17.1.1.1 / 255.255.0.0
	m1/3	217.1.1.1 / 255.255.0.0
	m1/4 (50C-port2)	18.1.1.1 / 255.255.0.0
	port1	192.168.16.230 / 255.255.255.0
	port2	10.58.100.99 / 255.255.255.0
	port3 (40C_port1)	27.1.1.1 / 255.255.0.0
	port4	29.1.1.1 / 255.255.0.0
	port5	37.1.1.1 / 255.255.0.0
	port6	38.1.1.1 / 255.255.0.0
	port7	117.1.1.100 / 255.255.0.0
	port8 (Server P2)	118.1.1.100 / 255.255.0.0

N)



## 3.2 开启代理

进入到 m1/2 口下将接口的 ip 地址改为和拓扑图一致并将 web 代理开启:

接口名称	m1/2 (00:60:E0:67:72:B9)					
别名	50C-port1					
连接状态	已启用					
地址模式	为CI	ient端的网主	<b>é地址</b>			
●自定义 ○ DHCP	DEPOF					
IP地址/子网掩码:	17.1.1.1/255.255	.0.0				
IPv6地址:	3ffe:1:7:1::1/64					
开启端口监控功能	-					
☑ 开启显式Web代理功能						
□ 开启IPMAC绑定功能	-2					
启用DDNS						
□ 分解大于MTU的输出包.	1500 (字节)					
☑ 启用DNS查询	recursive ~					
	HTTPS	PING	⊡нттр			
管理访问	⊠ ssh		TELNET			
	WEBAPI-HTTP	WEBAPI-HTTPS	5			
	HTTPS	PING	⊡нттр			
IPv6端口访问权限	⊠ssн					
			5			
た測服条器						
た調査が必						
印店						
1人国	0					
链路超载附值	0	KBps				



## 3.3 添加附加 ip 地址

m1/2 (00:60:E0:6	7:72:B9)		m1/2 (00:60:E0:6/:/2:B9)						
50C-port1									
已启用									
PPPOE									
掩码: 17.1.1.1/255.255.0.0									
3ffe:1:7:1::1/64		- 172 							
1500 (字节)									
recursive ~									
	PING	Инттр							
⊠ ss <mark>H</mark>									
WEBAPI-HTTP	WEBAPI-HTTPS	5							
HTTPS		Инттр							
⊠ssн									
WEBAPI-HTTP	WEBAPI-HTTPS	5							
Ping TCP F	Echo 🗹 UDP Echo								
0									
	DPPPoE 50C-port1 已启用 17.1.1.1/255.255 3ffe:1:7:1::1/64 1500 (字节) recursive ~ ☑ HTTPS ☑ SSH ☑ WEBAPI-HTTP ☑ HTTPS ☑ SSH ☑ WEBAPI-HTTP	SOC-port1 三倉用 DPPPoE 17.1.1.1/255.255.0.0 3ffe:1:7:1::1/64 1500 (字节) recursive ✓ ☑ HTTPS ☑ PING ☑ SSH ☑ SNMP ☑ WEBAPI-HTTP ☑ WEBAPI-HTTPS ☑ HTTPS ☑ PING ☑ SSH □ SNMP ☑ WEBAPI-HTTP ☑ WEBAPI-HTTPS ☑ HTTPS ☑ PING ☑ SSH □ SNMP ☑ WEBAPI-HTTP ☑ WEBAPI-HTTPS	SOC-port1         已用用         PPPoE         17.1.1.1/255.255.0.0         3ffe:1:7:1::1/64         1500 (字节)         recursive         ✓						



HTTP 正向代理配置手册

	编辑接口		
IP地址 / 子网掩码: ☑ 检测网关的接口: 检测服务器	17.2.1.1/16 <del>状</del> 况	为client端子网2的网关地 址	ł
检测协议		CP Echo UDP Echo	
管理访问	□ https □ □ ssh □		
	ок	取消	

进入到 m1/4 口下,设置方法和设置 m1/2 的一致:

接口名称	m1/4 (00:60:E0:67:72:BB)	
别名	50C-port2	
连接状态	已启用	

#### 地址模式

●自定义 ○ DHC		
IP地址/子网掩码	18.1.1.1/255.255.0.0	为Server的网关地
IPv6地址:	3ffe:1:2:2::1/64	址

开启演口些培劢能	-			
☑ 开启显式Web代理功能				
□ 开启IPMAC绑定功能	-			
□ 启用DDNS				
□ 分解大于MTU的输出包.	1500	(字节)		
☑ 启用DNS查询	recursive	~		
	Øнттрѕ		PING	Инттр
管理访问	SSH			TELNET
	WEBAPI	I-HTTP	WEBAPI-HTTPS	





接口名称 m1/4 (00:60:E0:67:72:BB)					
别名	50C-port2				
连接状态	已启用				
地址模式					
●自定义 ○ DHCP (	PPPOE				
IP地址/子网掩码: 18.1.1.1/255.255.0.0					
IPv6地址:	3ffe:1:2:2::1/64				
□ 开启端口监控功能					
☑ 开启显式Web代理功能					
□ 开启IPMAC绑定功能					
□ 启用DDNS					
□ 分解大于MTU的输出包.	1500 (字节)				
☑ 启用DNS查询	recursive ~				
	HTTPS	PING	<b>⊴н</b> ттр		
管理访问	⊠ssн				
	WEBAPI-HTTP		5		
	HTTPS	PING	<b>⊡н</b> ттр		
IPv6端口访问权限	⊠ ssh				
	WEBAPI-HTTP		5		
☑检测网关的接口状况					
检测服务器					
检测协议		cho 🗹 UDP Echo			
权值	0				
链路超载阀值	0	KBps			
	1.1				



### 3.4 网络代理的设置

KFW	监控▼	系统管理-	路由▼	防火墙▼	病毒与攻击▼	上网行为管理
系统管理 / 网络 / 接口		控制面板	<u> </u>			
1500		网络	<b>&gt;</b>	接口		
□ 开启IPMAC绑定功能 □ 启用DDNS		DHCP服务器	R >	X		
□ 分解大于MTU的输出包.	1500	配置	•	选项		
☑ 启用DNS查询	recursiv	管理员设置	1	DNS 服务	5 <u>8</u>	
管理访问	⊠ HTTP ⊠ SSH ⊠ WEBA	证书 维护 PI-TITE EDV		网络代理 Maineline		
IPv6端口访问权限	⊠ HTTPS ⊠ SSH ⊠ WEBAI	₽ Ωs PI-HTTP Øv	'ING NMP VEBAPI-HTT		r	



下图序号 1 中的 m1/2 和 m/4 接口开启 web 代理后会在此处显示监听; 序号 2 中的端口号可以是任意,默认是 80;而 8080 也比较常用; 序号 3 中选择阻止;(如果选择放行下一步将不需要设置,直接跳过即可)

显式Webf	<b>:理选项</b> 常规设	置(显式Web代理和透明Web缓存)
启用显式Web代理		S FTP PAC
在接口上监听 1	m1/2, m1/3, m	1/4, port4, port7, port8 🛕 📝
нттр端口 2	8080	
HTTPS端口	0	(置0以使用HTTP端口)
FTP端 <mark>口</mark>	0	(置0以使用HTTP端口)
PAC端口	0	(置0以使用HTTP端口)
PAC文件内容	ß	
未知HTTP版本	尽力处理	~
认证识别符	default	
默认防火墙动作	● 放行 ● 66	

### 3.5 添加策略

在防护墙中添加允许策略:(防火墙的默认策略是全部阻止)

监控▼	系统管理→路由→	防火墙-	病毒与攻击	▼ 上网行为管理	VPN-
		策略	•	策略	
會删除	1↓移动到 ● 插入 -	1 地址	•	显式NAT表	
	▼序号	服务		DDoS策略	
> m1/4(	(50C-port2) (1)	时刻表		探测策略	
> m1/2(	(50C-port1) (1)	流量整形器		IPv6策略	
4(50C-p	ort2) (1)	虚拟IP	8	协议选项	
		负载均衡			
		IPMAC绑定	•		

netitest.com		1			的代生化重丁加
KFW	监控▼	系统管理,	• 路由	▼ 防火	墙▼ 病毒
方火墙 / 策略 / 策	略				
创建, 🖌 编辑	1 - 自胆除	11 移动到	•0 插入	冒 检査	
		▼序号			T 2
方火墙 / 策略 / 策	瞻	C port1)	1		
防火墙/策略/策	赠 [m1/2(50	)C-port1)	]		~
山 防火墙 / 策略 / 第 源接口/区 源地址	略 m1/2(50 all	)C-port1)	]		 ▼ ■多遊
山 防火墙 / 策略 / 第 源接口/区 源地址 目的接口/区	略 m1/2(50 all m1/4(50	OC-port1) OC-port2)	]		✓ ● 国参送 ●
防火墙 / 策略 / 策 源接口/区 源地址 目的接口/区 目的地址	略 m1/2(50 all m1/4(50 all	OC-port1) OC-port2)			✓ ■ ■多遊 ▼ ■ ■多遊
防火墙 / 策略 / 第 源接口/区 源地址 目的接口/区 目的地址 対刻表	略 m1/2(50 all m1/4(50 all always	DC-port1) DC-port2)	]		✓ ■多遊 ▼ ■多遊 ▼ ■多遊
防火墙/ 策略/ 第 源接口/区 源地址 目的接口/区 目的地址 时刻表 服务	贈 m1/2(50 all m1/4(50 all always ANY	OC-port1) OC-port2)	]		<ul> <li>✓</li> <li>✓</li></ul>

源接口/区	m1/4(50C-port2)	~
源地址	all	- ■多选
目的接口/区	m1/2(50C-port1)	~
目的地址	all	▼ ■多选
时刻表	always	~
服务	ANY	▼ ■多选
动作	ACCEPT	~



防火墙/策略/策略

HTTP 正向代理配置手册

朝接口/区	web代理	$\sim$
原地址	all	- ■多选
目的接口/区	m1/4(50C-port2)	~
的地址	all	▼ 5500000000000000000000000000000000000
が乍	ACCEPT	~

□ 启用基于BYOD用户认证的策略

#### 最后的效果如下:

0 00k - / 191	Ⅰ• 自删除 11 移动到 ● 插入	雪 检查				( E183	1) ④ 基于接口查看 〇 清单式查!						
	▼扇号	<b>工 路地址</b>	▼ 目的地址	T 时刻表	T 185	て动作	▼状态						
r m1/2(50C-port1) -> m1/4(50C-port2) (1)													
	2	o all	o all	always	o ANY	ACCEPT							
▼ m1/4(50C-por	m1/4(50C-port2) -> m1/2(50C-port1) (1)												
	3	o all	o all	always	ANY	ACCEPT							
▼ web-proxy -> i	• web-proxy -> m1/4(50C-port2) (1)												
	18	• all	o all	always		ACCEPT							
N 即形(1)													

### 4. 设置 Supernova 测试仪

### 4.1 HTTP 的正向代理实例

1)登录系统,依次点击,用例->代理设备测试->HTTP->新建服务->增加,单 击增加,在弹出的选择用例选项中,编辑用例网络选项,根据需要修改配置 参数,然后点击确定,进入用例配置页面。





2)点击确定,进入用例配置界面,配置子网信息。

客户端			over 19 19 19 19 19 19 19 19 19 19 19 19 19	服务端			
0 就用跳口			MAC 90:e2:ba:ee:92:50	⊘ 就用跳口			MAC 90:e2:bared
CPU核绑定			-	CPU核绑定			
报文捕获			•	报文编获			
MAC设置			•	MAC设置			
QinQ (IIIIII)			-	QinQ (30/8)			
子网 🛛			+ 添加子网	子网 😡			+ 18107
第1个子网			8 移除子内 ② 第用子列	第1个子网			8 修辞子列 ② 美用子
	测试仪端口IP地址或范围	17.1.2.2.17.1.2.201	测试仪模拟客户端的使用的	匀IP	测试仪端口IP地址或范围	18.1.1.100	◎服务器端的IP
	测试仪第口子网接码	16			测试仪端口子网掩码	16	0
	透视路由器	17,1.254.1			送找路由器	20.1.254.2	
	影战仪第口网关	17.1.1.1			游试仪前口用关	20.1.1.1	0
	VLAN ID	1			VLAN ID		
	代理服务IP地址	17.1.1.1			子网模拟	只模拟服务讲	v
	子网横拟	只變以客戶演 🗸 🚺	火墙与测试仪客户端port口	相连的开启webi	E向代理的接口IP		
	服务制作在主机	192.168.16.237					
	服务编所在演口	port3					
	服装建筑在子园	第1个子段					
	oncerner (CL 7 PS						

### 4.2 启动实例

用例参数配置中选择正向代理:

用例名称	HttpCps_P	noxy_admin_2021	10120-14:27:13 - / _ (不支持中文)	寺間)		朝鮮式型子を(相当55年5) 0 [: 10]: 0 時代で在当社団の16(「南山田市水・朝鮮式四16(<市山田市水・朝鮮式ロ50-9-1-147)					
<b>网络 参数</b>	限速	套户端	18.95 <b>8</b> 8	记录							
				用户admin占用	9荐 60	GB					
				用例运行占用	用Padmin即请点用的内容 77 60	2盘。可以到资源一内存管理页面由请 GB					
					並行此用例占用的內存至何。	包括OPOK的大型均存。以及SSL最低合用的	南部通道派统内容, 25圈: 2-60GB				
				DPDK大页内在	SHE 50 DPDK大页内存占用例运行内	%€ 用約四分比、运行HTTPS并发用例时、建议	K页内存占比50%,剩余内存用于提	位551.余质,范围: 30%、95%			
				出现用户	2 <b>56</b>						
				新建油料	范囲: 1・16,384, 明介留/= (数 0	调何口和CPUHE、至少要有一个通知用户					
					每个CPU技術建TCP连接的》	我、0表示无限制					
				请求)&ZDHos	FR た HTTP请求5-20中、景宮告記	「 図ADHost学校、 配配正式HCREADPAR名を注意	0.0015-02				
				HTTPHO	記念で	~					

选择代理端口号:

用例案称 HttpCps_Proxy_admin_20210120-	14:27:13	御成即任(同分)(1) 0: 10: 0
他注乎何类型: A-Z/a-z/0.9/:1-/_(A)	2394-3244-9)	3月17日至此回日时,10日日期,19月17日)12日,中国日本11日日,19月17日)13日 13日日日日月日日日日日日日日日日日日日日日日日日日日日日日日日日日日日
网络 参数 限速 富户端 服	19日本 (記录)	
нттрод		
	源論口范围	10006-8535
		7000-1.000-65.535
	代理成负载设备纳口	8880 设置代理端口与防火墙HTTP代理端口号一致
		708. 0 - 65.535
	春户鸽关闭模式	Reset
		TCP與母產團的方式,可以使fin三階層時,也可以加速設eset能交易可
	HTTP请求其	User-Agent: Firefox/41.0
		la.
		* SollPLOSTIR发展是ison特区。 源在读水头中提出Content-Type: application/son * SollPLOSTIR发展是输出交流,请在读水头中提出Content-Type: application/x-www-form-urlencoded
	又件对象	
	27 III (c) 10	
	安徽列地	
		IN THE POST (\$1649 HERCENFIER, FOLKERFIER, FOLKE
		altara) fikelar
<b>_</b>		
▶ 北方网测到壮方四	티사크	笠10百 廿 1 <b>5</b>
	1.2 / 2 - 1 1	



配置报文捕获查看用例运行报文交互过程:

用例	名称 HttpCps_Proxy_admin_20	210120-14:27:13			测试时长 (时分秒)	0 :	10 : 0		
网络参数	限速 客户端	服务器 记录	1			abdiggerteeninges, mager	CT9868(2019) 45		
19:2	1	1							81 <b>1</b> 13
□端					服务端				
rt2					port6				
(用))(口)				MAC 68:91:d0.63:47:65	◎ 禁用読口				MAC 68:91:d0:63
PU核绑定				•	CPU核绑定				
<b>纹捕获</b>					报文捕获				
	协议类型	全郎	~			协议类型	全部	~	
		请选择协议的类型,无表示不由J	19769				请选择协议的类型,无表示不启则抓	8	
	IP地址					IP地址			
		源P地址或著目的P地址,例如1	7.1.1.2				源P地址或者目的IP地址,例如17.1.	1.2	
	Surger Contraction of the second seco	20141710201010000000, 005180				調日	源端口北京月め端门、60180		
	Pcap文件大小					Pcap文件大小	1		
		pcap文件大小、0 - 2000MB (既认	)				pcap文件大小、0 - 2000MB (徽以)		
	捕获包数	50000				捕获包数	50000		
		(悠園): 0 - 6000000 (新认)					范围: 0 - 6000000 (戴认)		
率与MAC				•	速率与MAC				
inQ (##/8)				•	QinQ (##///)				
网 0				+ 激加子网 🔺	子网 😡				+ 181071
个子网				會移除子同 ◎ 禁用子司	第1个子网				會移除子网 ② 葉用き
	测试仪端口IP地址或范围	17.1.2.2-17.1.2.200	0			测试仪第口IP地址或范围	18.1.1.100	0	

## 4.4 启动后正常运行界面

用例编辑保存后,点击运行按钮运行测试用例

<b>◎</b> 网测科	支 m	÷	28 NSR	200 2012	<b>後</b> 海 服告	Kite adm	lin			V20.12.06	Supernova-88			
■ 网关设备测试 Θ	0	HTTP新建	rpinse .											
• Regiment •		花取受到设备新	R教授局後期運行TP会会の最快速度、単今会和局中建立一般TPS運動、另分一次発動的TTPS運動(後送表明和限制の)、最后共活動員、再発達TPS連時共会合っ次規範がTTP会会。											
HTTP/HTTPS/HTTP2														
> HTTP		用例列表												
<ul> <li>新建設务</li> <li>并发展务</li> <li>美学新名</li> </ul>	0	+ 1820	8 89								₿ 8) 2 88			
> 香吐服务		□ #8	LEAST PARA	任务列表	用户	名字		99162	克隆	详细化加	导出 历史记录			
► HTTPS			×.		admin	HttpCp	s_Proxy_admin_20210120-14-27:13	1	伦		<b>R</b> 0			

#### 用例运行监控数据页面:

HTTP新聞 激成用户: adr	nin 用例名称: <u>HttpCps_Proxy_adm</u>	in_20210120-14-27:13					
走结果		altata maannaa			网络层		
22.168.16.228 - Port2	80	( down			参和 单语 多语 广播		
TTP #500 REE	3.520	短用最		<b>^</b>			
2.168.16.228 - Port6	1900	总和 port2 port6			192.168.16.228 - Port2	691	
TP_新建選系	0				NCCINC	10,560	1
			砂值	28	190,4,50,50,000,000,000	10.560	
		HTTP_新建選率	3,520	55,210	192.105.10.225 - PORto	678	
		HTTP_请求遗案	3,520	55,466	TR.X.BNX		-
		HTTP_围在码2xx	0	23,964	mx.xxa	0	
		HTTP_周应码3xx	0	0			
		HTTP_国应码4xx	0	0			
		HTTP_国应码5xx	3,520	31,246			
		HTTP_请求中断	0	0			
		HTTP_SERSED	0	0			
100	•	HTTP_FHQ#102 (00%)		46.073	BBB		
		HTTP_EDJ4582 (0069)		2.503	and the second s		
2.168.16.228 - Port2	8.82	HTTP_編大和政治((2019)		3,015,365	184		
中影響包教量	50.000				192 168 16 228 - Port2		
字节数量	6.946.151	(managed)			192.100.10.220 - POPLE		
CHARGE CO.	(王県) 已经停止 (下職)	6編层 0		<b>•</b>	CLARMON .		
168 16 228 - Port6	45.20	创和 port2 port6		^	192 168 16 228 - Port6		
物態的教量	50.000				10-MisButy		
(字节数量	5.707.198		ea	总数	22.85 96 08		
Sint P	(TR) P4346+ (TR)	TCP_主动新建连接	3.520	55,466	FURENCE		
	Carrie (19)	TCP_主动建成连接	3.520	55,466			
		TCP。被动建成连续	0	23,964			
		TCP_当截主动并发数量		256			
		TCP。当前被动并发散量		0			
		TCP_主动FIN关闭成功		0			_
200	L	TCP_被动FIN关闭成功		23,964	用例管理		
		TCP_主动Reset关闭连接		55,210			
* 占	H SR	TCP_被动Reset关闭连接		0	用例名称	用户名称	运
8内存 53.09%	46.91% 64322 MB	TCP_重传报文数量	0	0	HttpCps_Proxy_admin_2021012	20-14:27:13 admin	TE
5p.70 00	81% 30556 MB	TCP_主动新疆平均时延(团秒)		135			





### 用例运行结束,可以点击下载报文查看用例运行中报文交互



#### 客户端报文:

文件(	· 编辑(E) 视题(V) 影神(G)	捕获( <u>C</u> ) 分析( <u>A</u> ) 统计	HS) 电话(Y) 无线(W) 工具(D) 帮助(H)						
4.1	0 0 0 0 0 0 0 0	*****	📃 Q Q Q II						
1 teg	stream eq 0								+沈达表 • 드 🖾
Ho.	Tine	Saurce	Destination	Frotosol	Length	Sre	aFort 1	Ostfort Info	
11	403 1.001414	17.1.2.2	17.1.1.1	TCP		62 1	10000	8080 10000 + 8080 [SYN] Seg=0 Win=65535 Len=0 MSS=1452 SACK PERM=1	
10	484 1.001445	17.1.1.1	17.1.2.2	TCP		62	8888	10000 8080 - 10000 [SYN, ACK] Seg-0 Ack-1 Win-5840 Len-0 MSS-1460 SACK_PERM-1	
-+	405 1.001458	17.1.2.2	17.1.1.1	HTTP		174 1	00001	8080 GET http://18.1.1.100/index_1bytes.html HTTP/1.1	
	406 1.001563	17.1.1.1	17.1.2.2	TCP		60	8080	10000 8080 * 10000 [ACK] Seg-1 Ack-121 Win-5840 Len-0	
-	2201 3.995211	17.1.1.1	17.1.2.2	HTTP		176	8888	10000 HTTP/1.1 200 OK (text/html)	
L,	2202 3.995216	17.1.2.2	17.1.1.1	TCP		60 1	10000	8080 10000 → 8080 [RST, ACK] Seg=121 Ack=123 Win=65535 Len=0	
			日的旧为正向	代理服务器ID 1	7111				
۲			EID0 /attro	10年00056月1111					>
> En	ano 405: 174 hytes on y	dre (1392 bits)	174 bytes cantured (1392 bits)						
> Et	hernet II. Spc: IntelCo	P PP:92:50 (90:P2	:ba:ee:92:50). Dst: AxionTec 67:72:bf	(00:60:e0:67:72:b	สา				
> 10	ternet Protocol Version	4. Sec: 17.1.2.2	. Dst: 17.1.1.1		-,				
	ansmission Control Prot	ocol. Src Port: 1	0000, Dst Port: 8080, Seg: 1, Ack: 1,	Len: 120					
~ Hy	pertext Transfer Protoc	0]							
2	GET http://18.1.1.100/	index 1bytes.html	HTTP/1.1\r\n						
	Host: 18.1.1.100\r\n Connection: keep-alive	(r\n 客户端	访问服务器IP 18.1.1.100						
	User-Agent: Firefox/41	.0\r\n							
	\r\n								
	[Full request URI: htt	p://18.1.1.100/inc	<pre>dex_lbytes.html]</pre>						
	[HTTP request 1/1]								
	[Response in frame: 22	81]							

