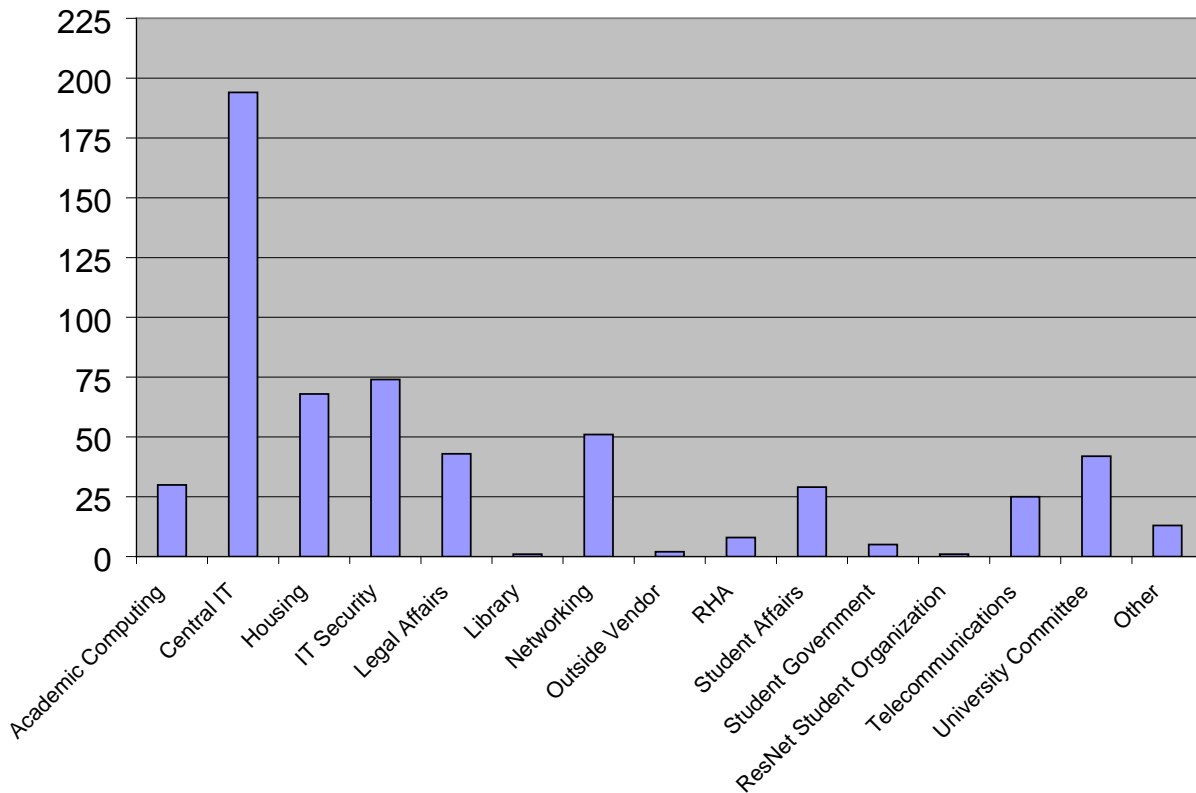


58. Who is responsible for setting policies governing your residential computer network? (Check all that apply)

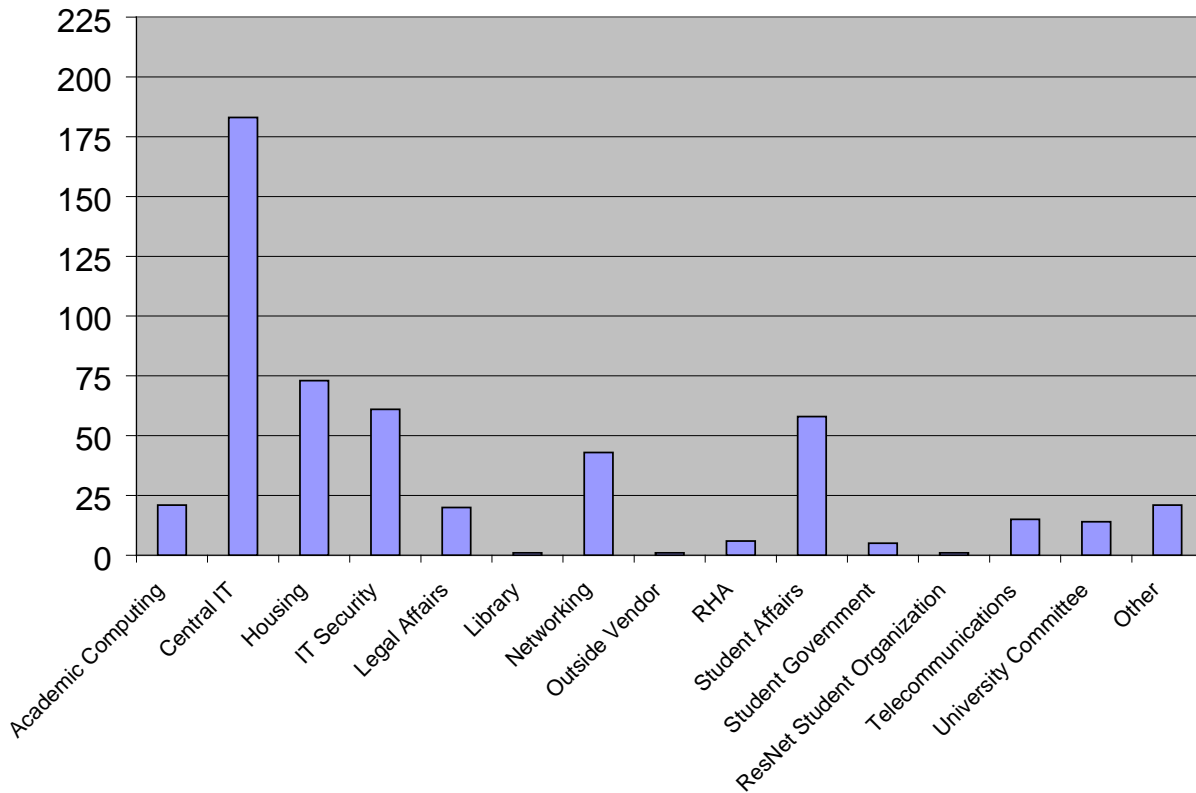
- Academic Computing
- Central IT
- Housing
- IT Security
- Legal Affairs
- Library
- Networking
- Outside vendor
- Residence Hall Association/Council
- Student Affairs
- Student Government (non-housing)
- Student organization specifically created for ResNet governance
- Telecommunications
- University committee(s)
- Other (please specify)



	Count	Proportion
Academic Computing	30	13%
Central IT	194	87%
Housing	68	30%
IT Security	74	33%
Legal Affairs	43	19%
Library	1	< 1%
Networking	51	23%
Outside Vendor	2	1%
RHA	8	4%
Student Affairs	29	13%
Student Government	5	2%
ResNet Student Organization	1	< 1%
Telecommunications	25	11%
University Committee	42	19%
Other	13	6%

**59. Who is responsible for enforcing policies governing your residential computer network?
 (Check all that apply)**

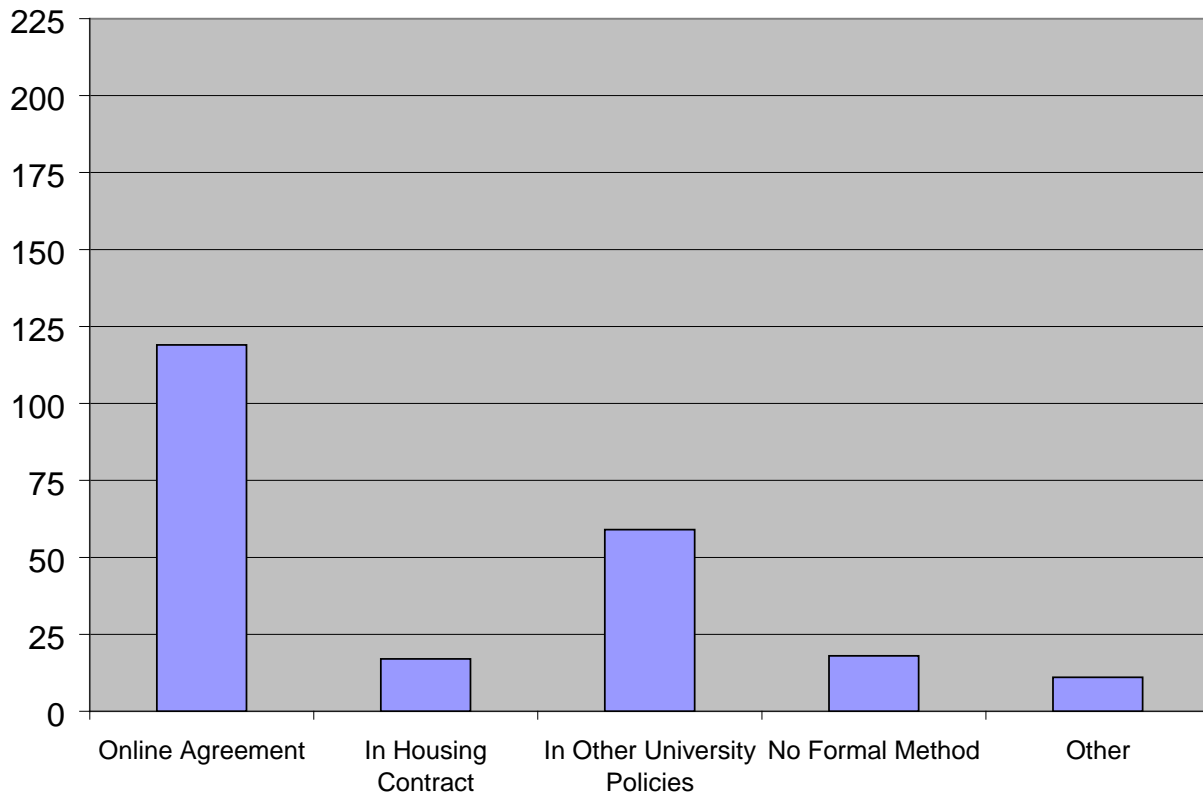
- Academic Computing
- Central IT
- Housing
- IT Security
- Legal Affairs
- Library
- Networking
- Outside vendor
- Residence Hall Association/Council
- Student Affairs
- Student Government (non-housing)
- Student organization specifically created for ResNet governance
- Telecommunications
- University committee(s)
- Other (please specify)



	Count	Proportion
Academic Computing	21	9%
Central IT	183	82%
Housing	73	33%
IT Security	61	27%
Legal Affairs	20	9%
Library	1	< 1%
Networking	43	19%
Outside Vendor	1	< 1%
RHA	6	3%
Student Affairs	58	26%
Student Government	5	2%
ResNet Student Organization	1	< 1%
Telecommunications	15	7%
University Committee	14	6%
Other	21	9%

60. How are residents required to confirm acceptance and knowledge of policies, restrictions, and requirements governing the use of the residential computer network?

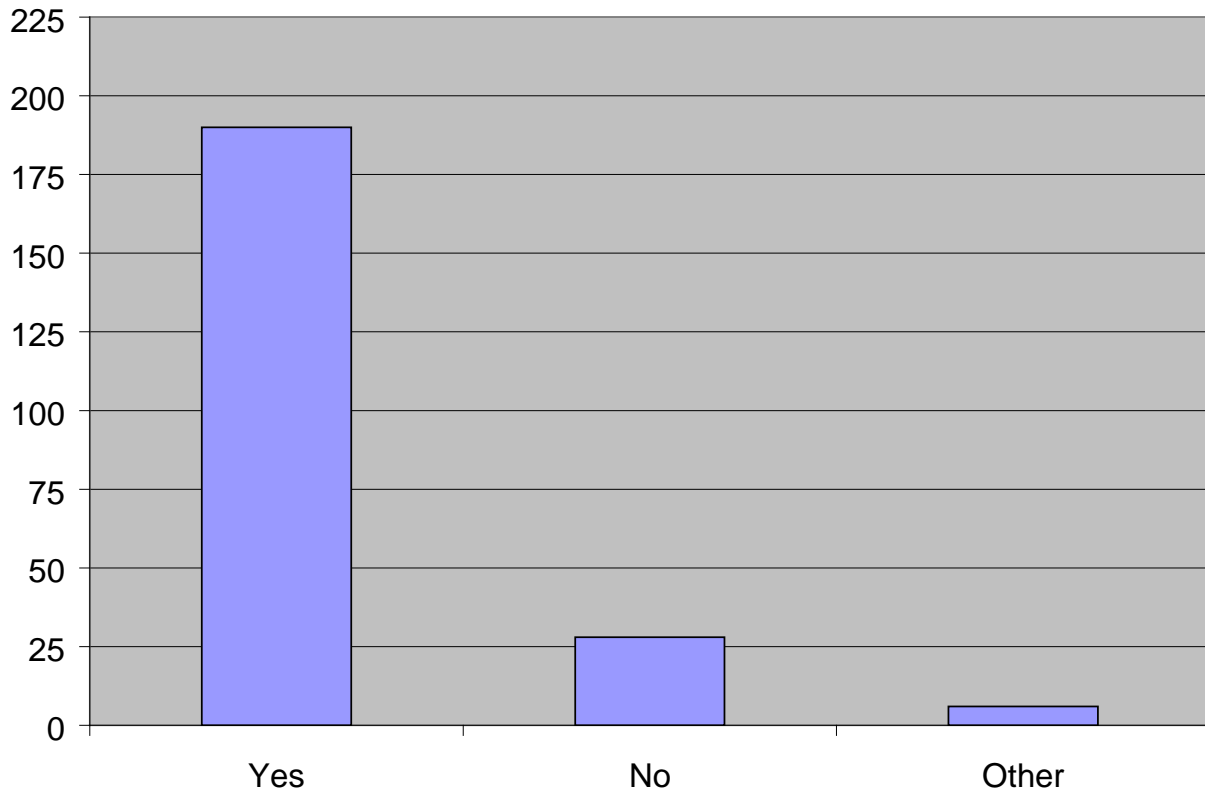
- Acceptance and knowledge of policies, restrictions, and requirements are required through an online agreement before the resident's connection is enabled
- Acceptance and knowledge of policies, restrictions, and requirements are part of the housing contract
- Acceptance and knowledge of policies, restrictions, and requirements are part of other university policies to which residents agree (admissions statement, computer usage agreement, etc.)
- There is no formal method
- Other (please specify)



	Frequency	Percent
Online Agreement	119	53%
In Housing Contract	17	8%
In Other University Policies	59	26%
No Formal Method	18	8%
Other	11	5%

61. Are any network services, ports, or protocols filtered, blocked, or otherwise restricted on your residential computer network?

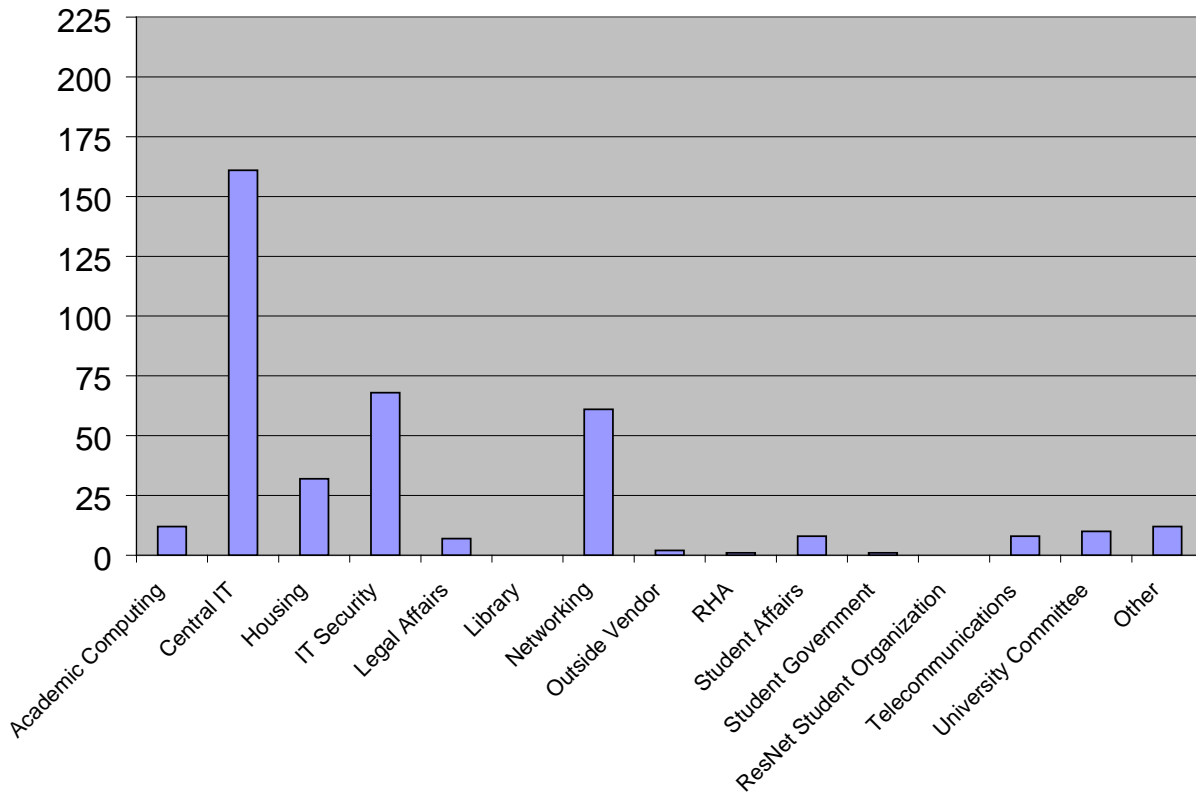
- Yes, we filter, block, or otherwise restrict activity on our residential computer network
- No, we do not filter, block, or otherwise restrict activity on our residential computer network
- Other (please specify)



	Frequency	Percent
Yes	190	85%
No	28	13%
Other	6	3%

62. Who determines which network services, ports, or protocols are filtered, blocked, or otherwise restricted? (Check all that apply)

- Academic Computing
- Central IT
- Housing
- IT Security
- Legal Affairs
- Library
- Networking
- Outside vendor
- Residence Hall Association/Council
- Student Affairs
- Student Government (non-housing)
- Student organization specifically created for ResNet governance
- Telecommunications

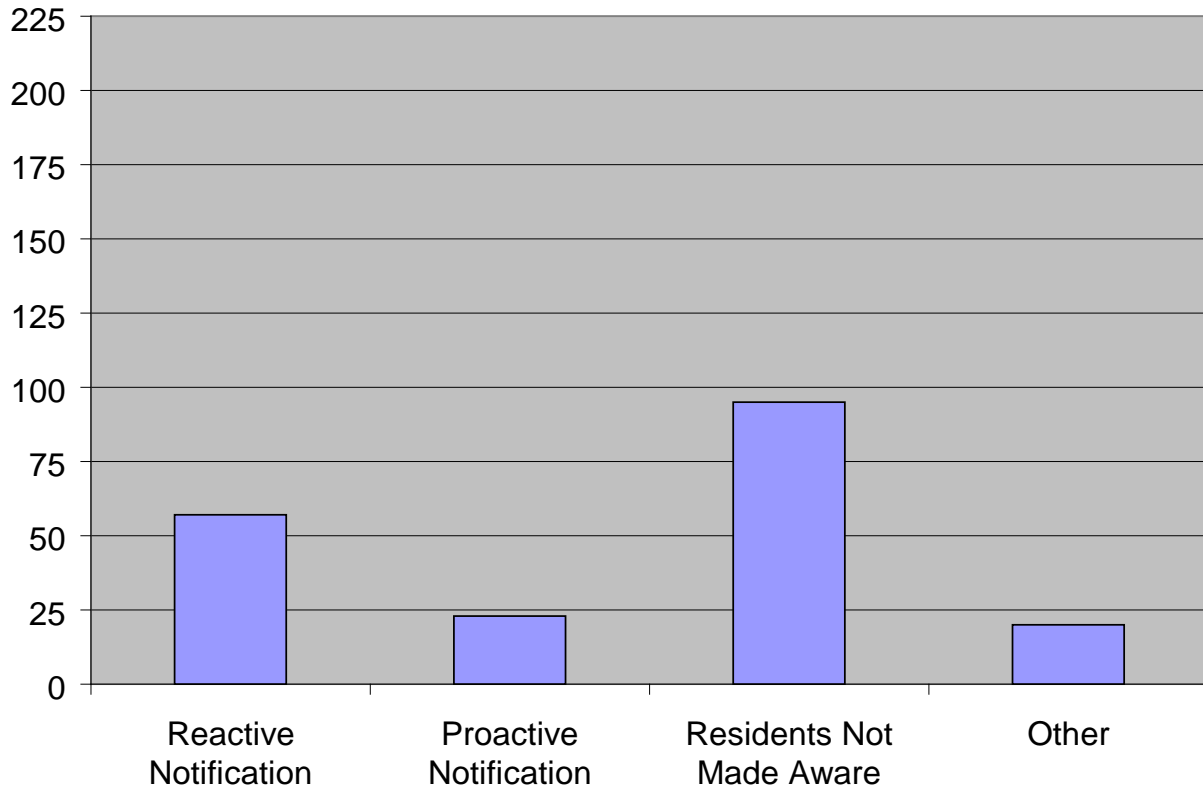


	Count	Proportion
Academic Computing	12	6%
Central IT	161	82%
Housing	32	16%
IT Security	68	35%
Legal Affairs	7	4%
Library	0	0%
Networking	61	31%
Outside Vendor	2	1%
RHA	1	1%
Student Affairs	8	4%
Student Government	1	1%
ResNet Student Organization	0	0%
Telecommunications	8	4%
University Committee	10	5%
Other	12	6%

28 respondents did not answer question 62 as they indicated in a previous question (61) that they do not block or filter services or ports.

63. Are residents made aware of network services, ports, or protocols which are filtered, blocked, or otherwise restricted?

- We are reactive - Residents are only made aware through mass communications (webpages, flyers, etc.)
- We are proactive - We keep residents aware of services, ports, and protocols that are filtered, blocked, or restricted on an on-going basis (for example, email sent directly to them)
- Residents are not made aware
- Other (please specify)

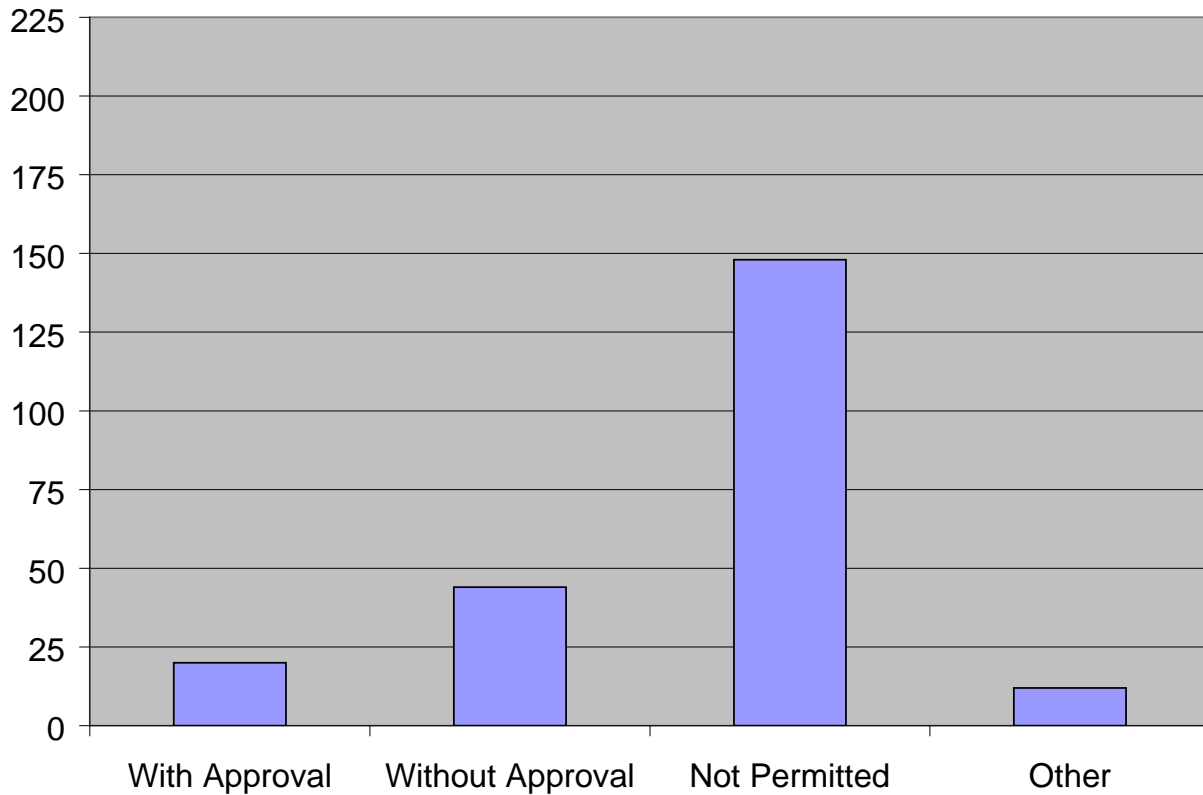


	Frequency	Percent
Reactive Notification	57	29%
Proactive Notification	23	12%
Residents Not Made Aware	95	48%
Other	20	10%
No Answer	1	1%

28 respondents did not answer question 63 as they indicated in a previous question (61) that they do not block or filter services or ports.

64. In general, are residents permitted to operate servers on the residential computer network?

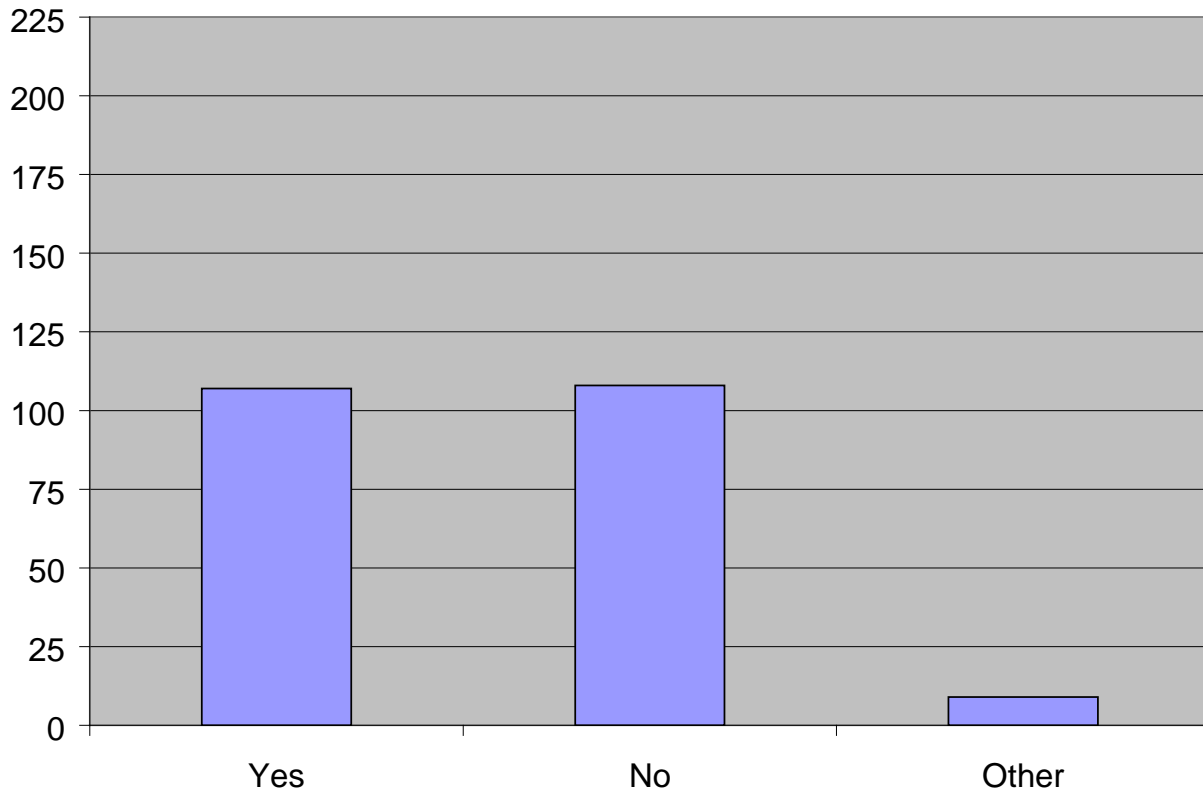
- Yes, residents are allowed to operate servers with prior approval or permission
- Yes, residents are allowed to operate servers without approval or permission
- No, residents are not allowed to operate servers
- Other (please specify)



	Frequency	Percent
With Approval	20	9%
Without Approval	44	20%
Not Permitted	148	66%
Other	12	5%

65. Is there a formal grievance or appeal procedure for violations of or challenges concerning policies and restrictions governing the residential computer network?

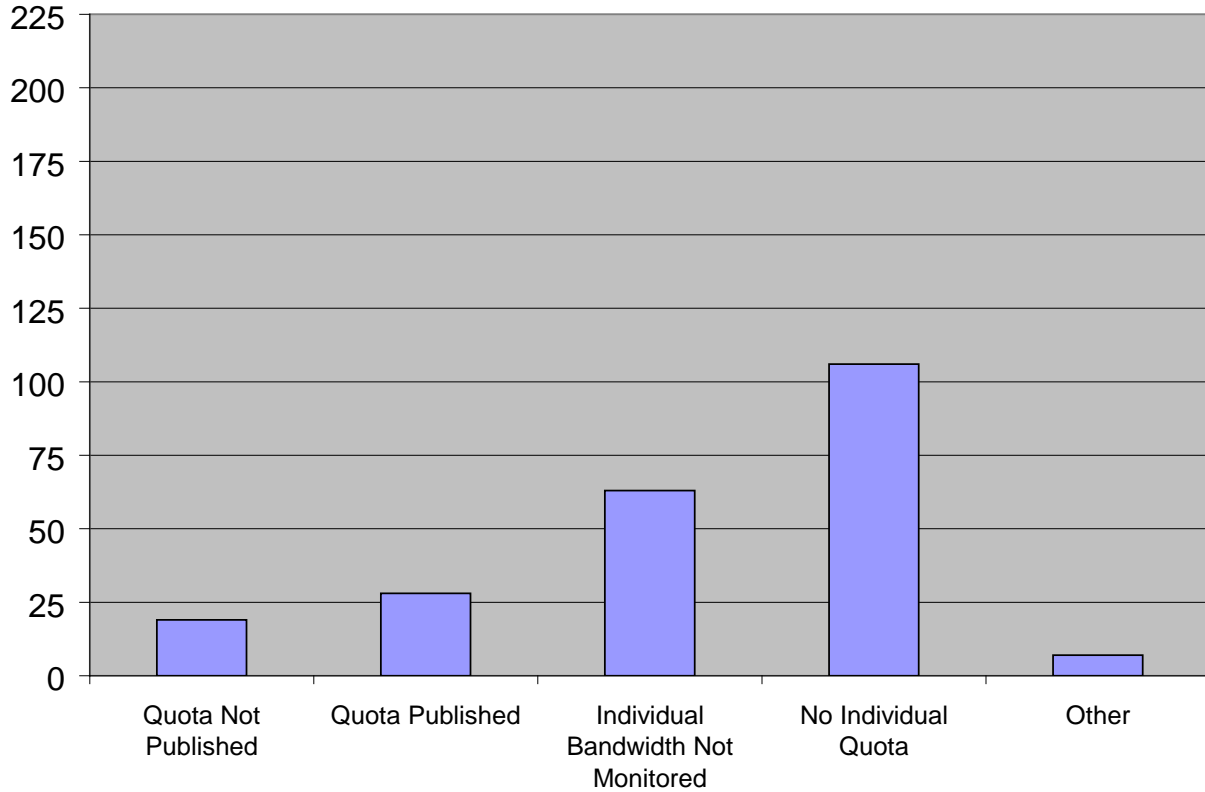
- Yes, we have a formal procedure
- No, we do not have a formal procedure
- Other (please specify)



	Frequency	Percent
Yes	107	48%
No	108	48%
Other	9	4%

66. Do residents have an individual bandwidth quota?

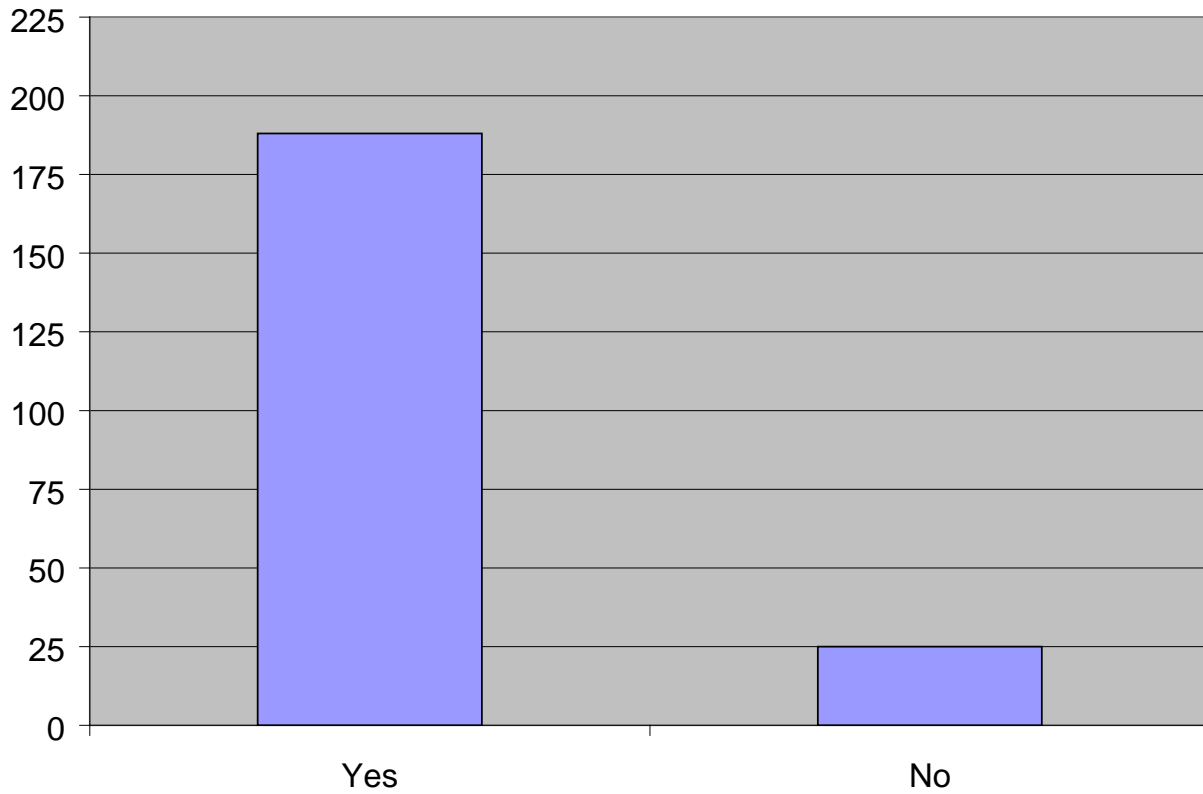
- Yes, we have a non-published quota for each user
- Yes, we have a published quota for each user
- No, we do not monitor bandwidth consumption on an individual level
- No, there is no set quota for individuals
- Other (please specify)



	Frequency	Percent
Quota Not Published	19	9%
Quota Published	28	13%
Individual Bandwidth Not Monitored	63	28%
No Individual Quota	106	47%
Other	7	3%
No Answer	1	< 1%

67. Does your campus practice packetshaping or other Quality Of Service (QOS) restrictions on the residential computer network?

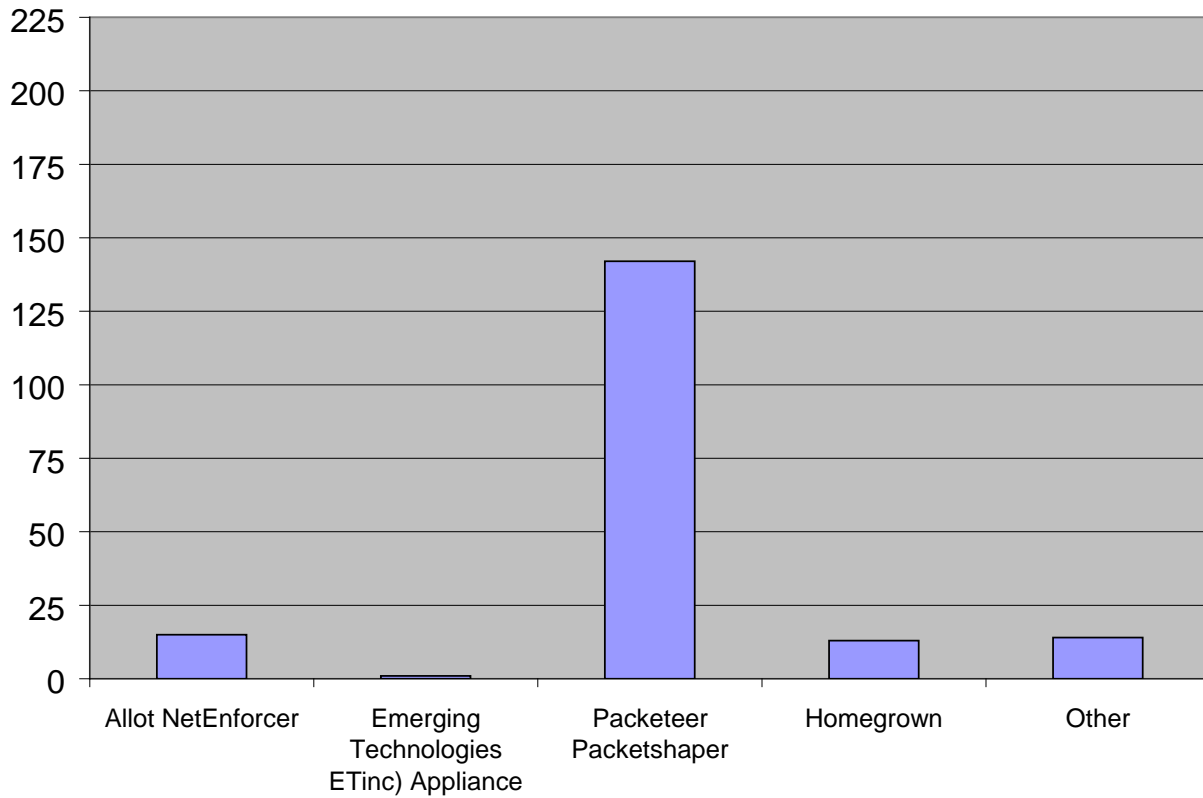
- Yes
- No
- Not sure



	Frequency	Percent
Yes	188	84%
No	25	11%
Not Sure	11	5%

68. What packetshaping or QOS product does your campus use?

- Allot NetEnforcer
- Checkpoint Floodgate-1
- Converged Networks (Sitara) QoSWorks
- Emerging Technologies (ETinc) Appliance
- Packeteer Packetshaper
- A "homegrown" (self-developed) product
- Other (please specify)

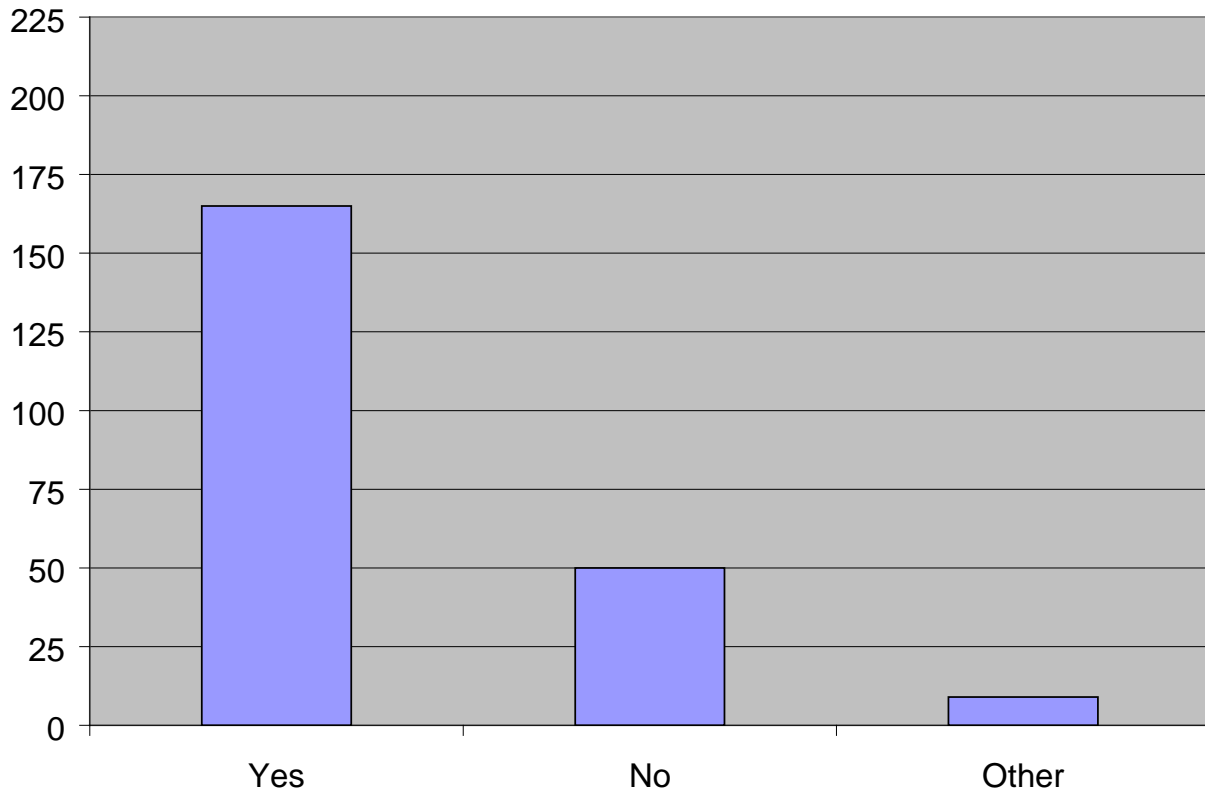


	Frequency	Percent
Allot NetEnforcer	15	8%
Emerging Technologies ETinc) Appliance	1	1%
Packeteer Packetshaper	142	76%
Homegrown	13	7%
Other	14	7%
No Answer	3	2%

36 respondents did not answer question 68 as they indicated in a previous question (67) that they do not practice packetshaping or Quality of Service (QOS).

69. Does your campus have an online registration process in place that requires residents to register their computer before their connection is fully functional?

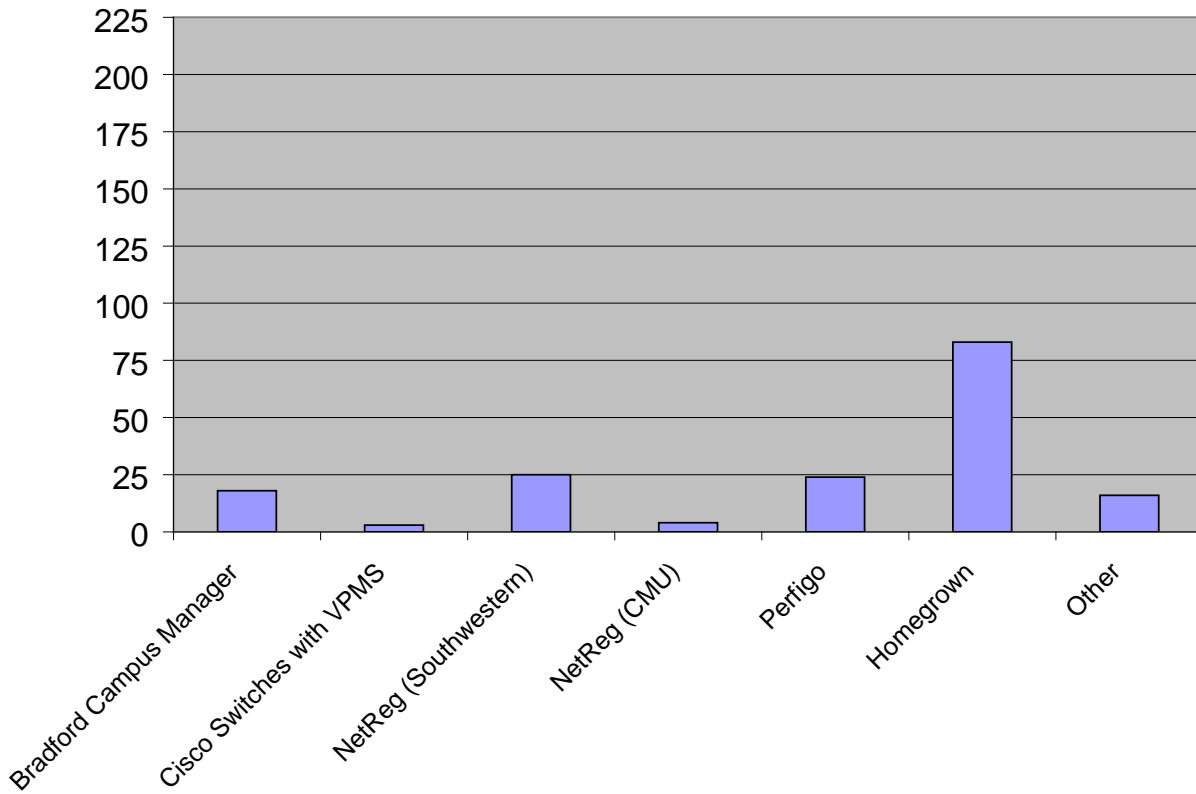
- Yes
- No
- Other (please specify)



	Frequency	Percent
Yes	165	74%
No	50	22%
Other	9	4%

70. Who developed your online registration process?

- Bradford Campus Manager
- Cisco switches with VMPS
- NetReg (www.netreg.org - Southwestern University)
- NetReg (www.net.cmu.edu/netreg/-Carnegie Mellon)
- Perfigo
- "Home grown" (i.e. developed in-house at your institution)
- Other (please specify)

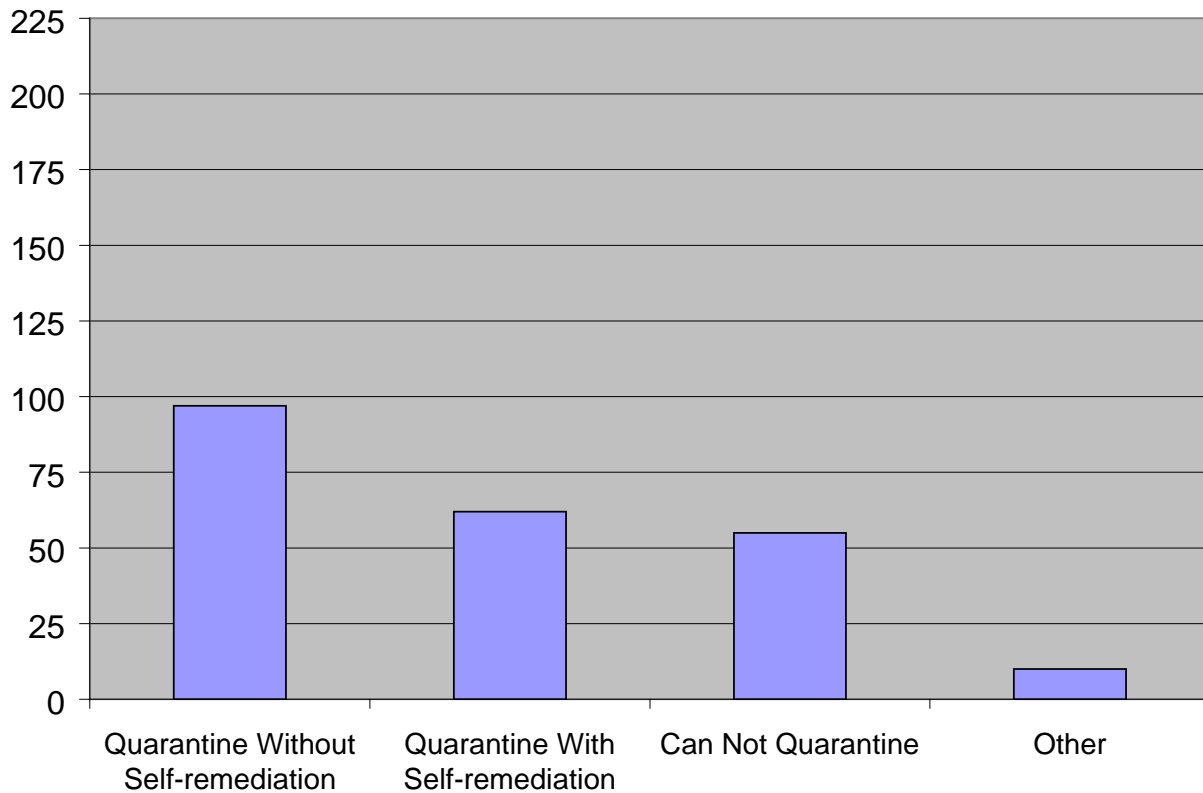


	Frequency	Percent
Bradford Campus Manager	18	10%
Cisco Switches with VPMS	3	2%
NetReg (Southwestern)	25	14%
NetReg (CMU)	4	2%
Perfigo	24	14%
Homegrown	83	48%
Other	16	9%
No Answer	1	1%

50 respondents did not answer question 70 as they indicated in a previous question (69) that they do not employ an online registration system.

71. Does your campus have a system in place on your residential computer network to automatically detect problematic (infected, unpatched, etc.) computers and quarantine them (to stop the spread of a virus, protect critically vulnerable computers, etc.)?

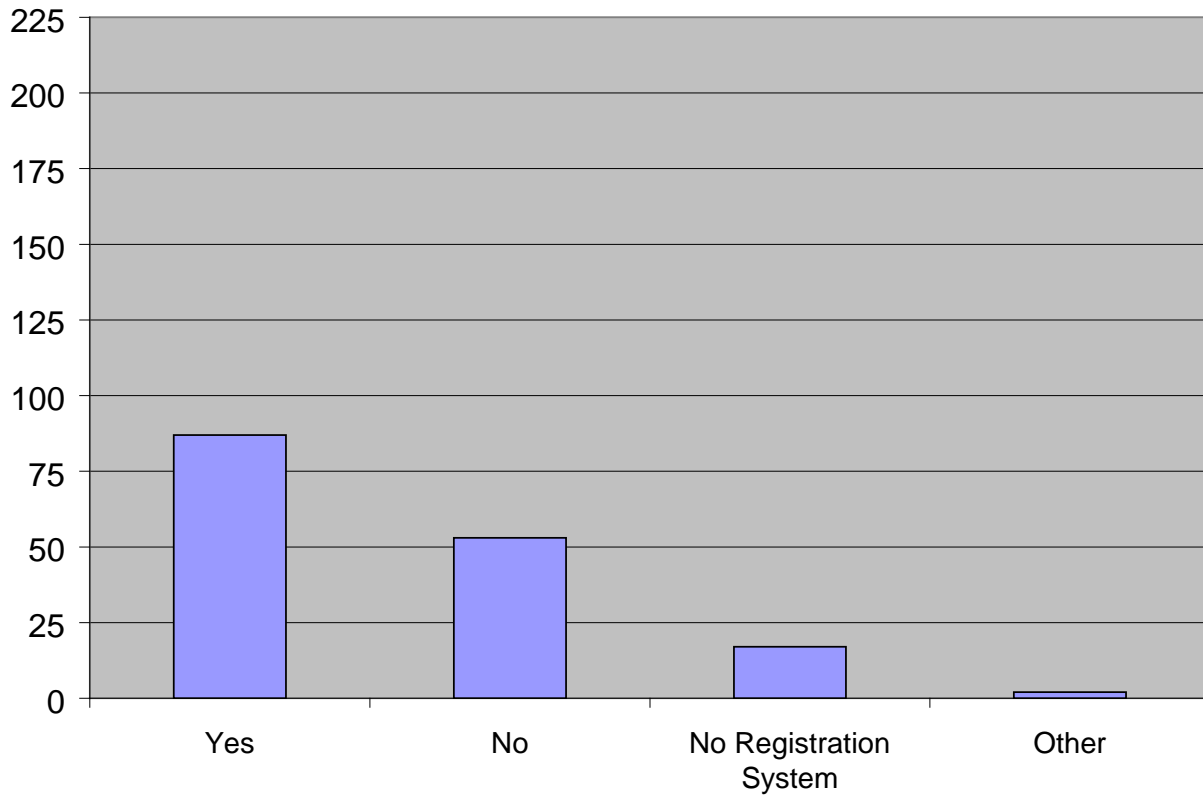
- Yes, we have the ability to quarantine problematic computers but no automated or self-remediation process
- Yes, we have the ability to quarantine problematic computers with an automated or self-remediation process
- No, we do not have neither the ability to isolate problematic computers
- Other (please specify)



	Frequency	Percent
Quarantine Without Self-remediation	97	43%
Quarantine With Self-remediation	62	28%
Can Not Quarantine	55	25%
Other	10	5%

72. Is your process integrated with an online registration system?

- Yes, our detection or isolation system is integrated with our online registration system
- No, our detection or isolation system is not integrated with our online registration system
- We do not have an online registration system
- Other (please specify)

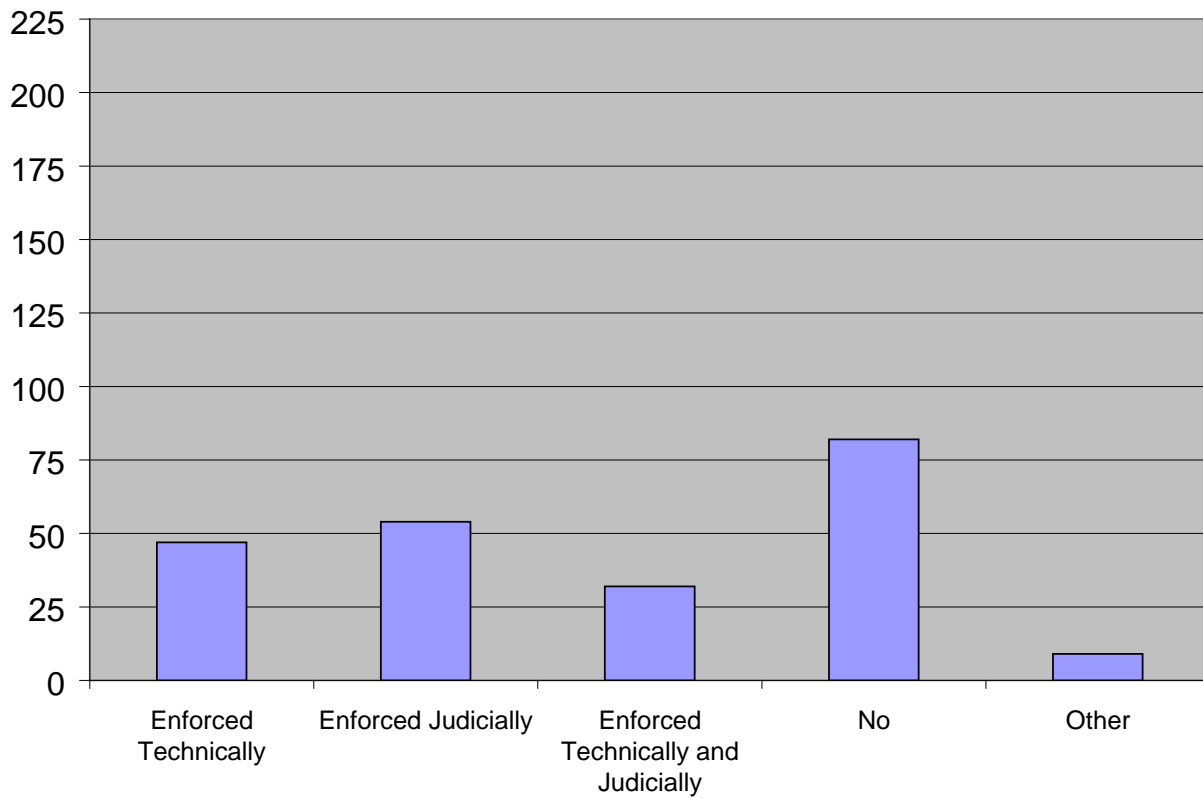


	Frequency	Percent
Yes	87	55%
No	53	33%
No Registration System	17	11%
Other	2	1%

65 respondents did not answer question 72 as they indicated in a previous question (71) that they do not employ a quarantine system.

73. Are residents required to install any security-related software on their computer before they can use the residential computer network?

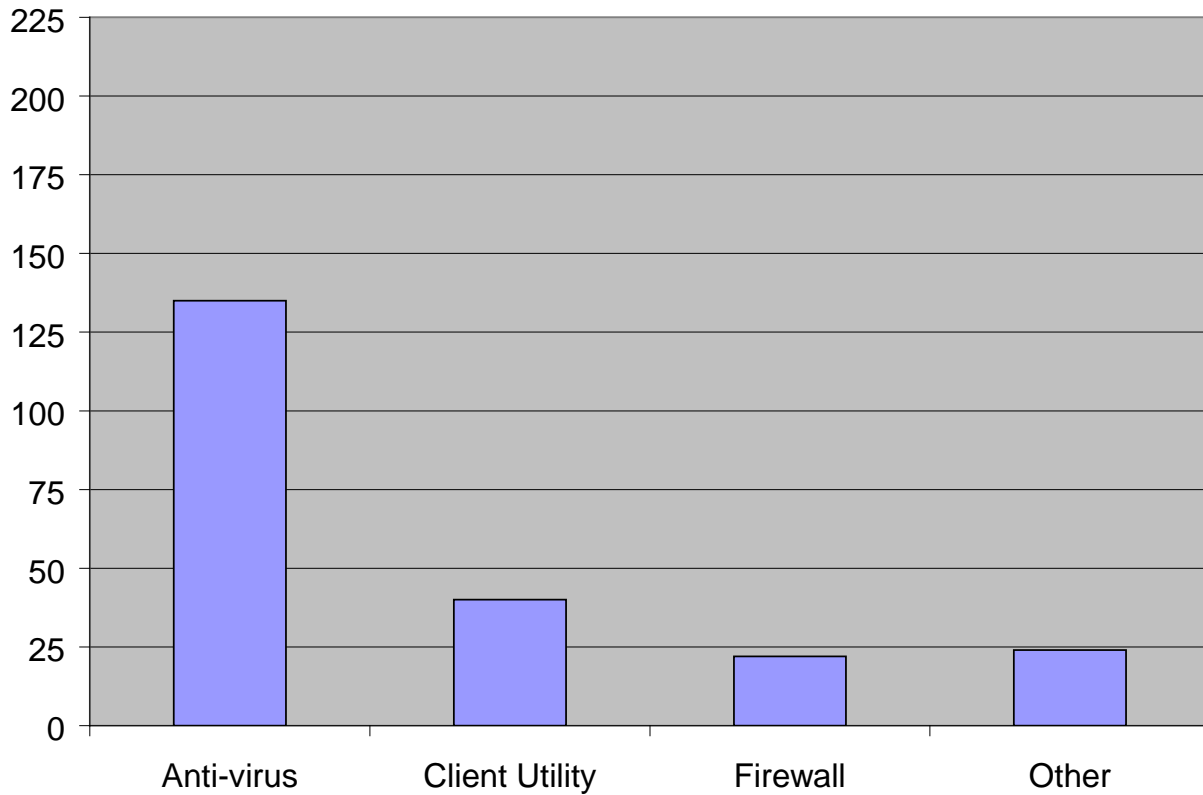
- Yes, residents are required to install security-related software and we enforce this primarily through technical measures
- Yes, residents are required to install security-related software and we enforce this primarily through non-technical (judicial or educational) policies
- Yes, residents are required to install security-related software and we enforce this through technical measures and non-technical policies
- No, residents are not required to install any security-related software to use the network
- Other (please specify)



	Frequency	Percent
Enforced Technically	47	21%
Enforced Judicially	54	24%
Enforced Technically and Judicially	32	14%
No	82	37%
Other	9	4%

74. What security-related software are residents required to install? (Check all that apply)

- Anti-virus software
- Client utility to verify settings, patch level, etc.
- Firewall
- Other (please specify)

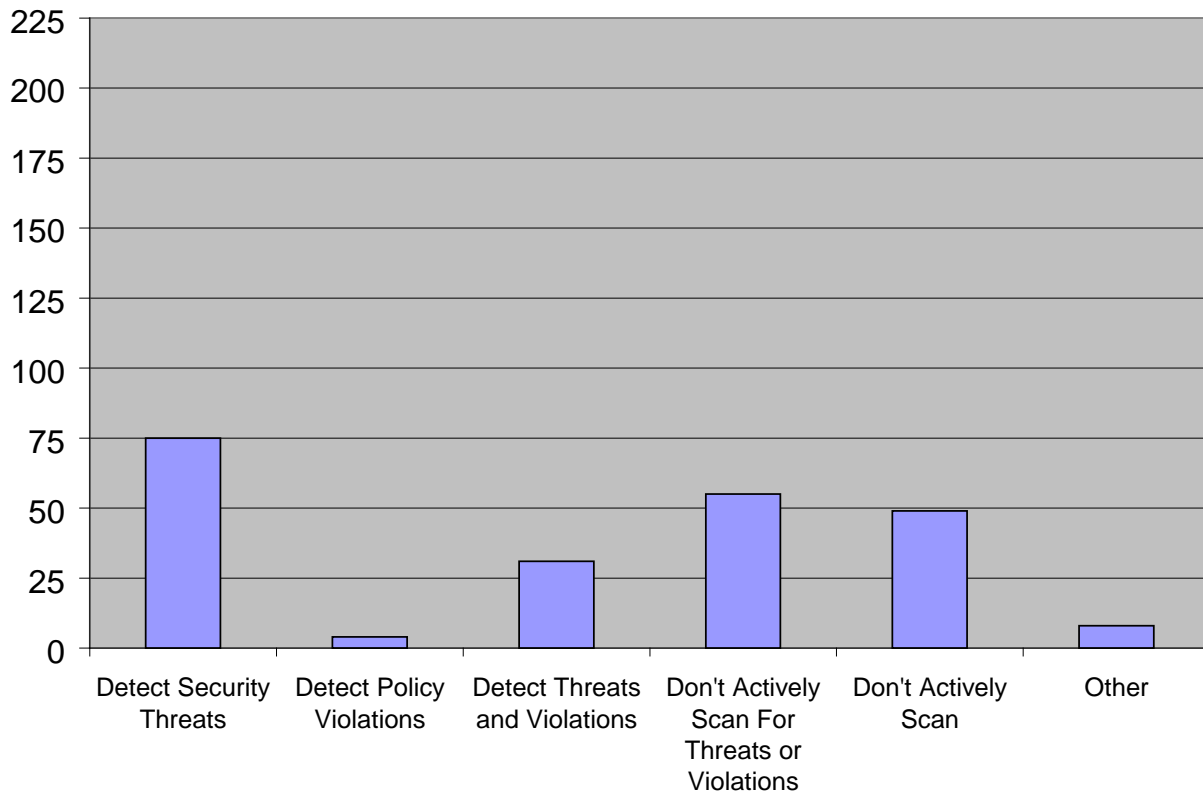


	Count	Proportion
Anti-virus	135	96%
Client Utility	40	29%
Firewall	22	16%
Other	24	17%

82 respondents did not answer question 74 as they indicated in a previous question (73) that they do not require residents to install security-related software. 2 additional respondents also declined to answer question 74.

75. Does your campus conduct active scans of the residential computer network to locate security threats or detect residents in violation of your policies and requirements?

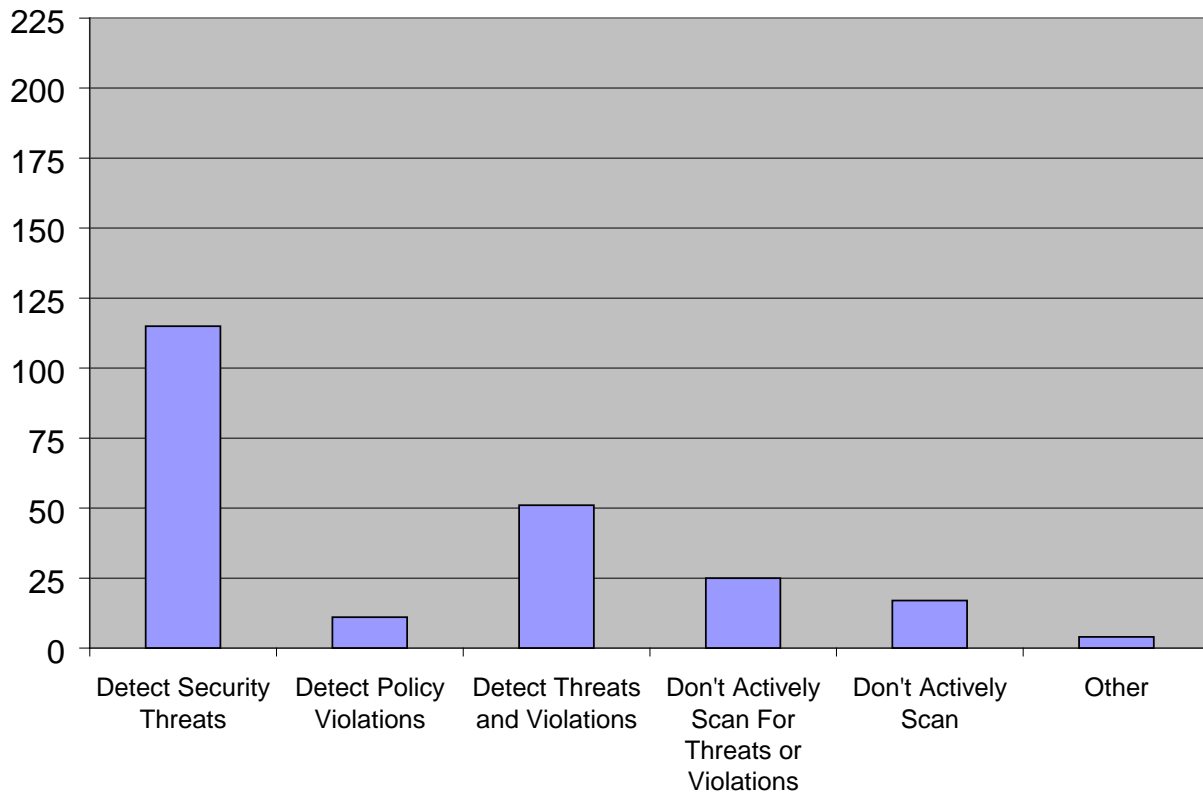
- Yes, we actively scan primarily to detect security threats
- Yes, we actively scan primarily to detect residents in violation of policies and requirements
- Yes, we actively scan to detect both security threats and policy violations
- No, we do not conduct active scans for these purposes
- No, we do not conduct active scans at all
- Other (please specify)



	Frequency	Percent
Detect Security Threats	75	34%
Detect Policy Violations	4	2%
Detect Threats and Violations	31	14%
Don't Actively Scan For Threats or Violations	55	25%
Don't Actively Scan	49	22%
Other	8	4%
No Answer	2	1%

76. Does your campus passively monitor the residential computer network to locate security threats or detect residents in violation of your policies and requirements?

- Yes, we passively monitor primarily to detect security threats
- Yes, we passively monitor primarily to detect residents in violation of policies and requirements
- Yes, we passively monitor to detect both security threats and policy violations
- No, we do not passively monitor network traffic for these purposes
- No, we do not passively monitor network traffic
- Other (please specify)



	Frequency	Percent
Detect Security Threats	115	51%
Detect Policy Violations	11	5%
Detect Threats and Violations	51	23%
Don't Actively Scan For Threats or Violations	25	11%
Don't Actively Scan	17	8%
Other	4	2%
No Answer	1	< 1%