



IPv6 and Firewalls
February 16, 2011

IPv6 and Firewalls

- @ Georgia Tech
 - IPv4 network
 - Early IPv6 network
 - Current IPv6 network
 - Future IPv6 network
- Issues
- Conclusions
- Extras and Discussion

IPv4

- Star configuration with multiple distribution routers
- Border firewalls
 - Campus wide policies, bogon filtering, etc.
- Unit Firewalls
 - Different firewall policies between campus units
 - Campus units manage their own policies, with advice from Information Security via custom application
 - One layer 2 firewall per subnet
 - Approximately 430 firewalls on campus
 - Primarily Cisco Firewall Services Modules (FWSM)

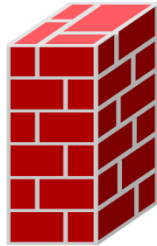
IPv4



Internet



Border Routers
*BGP external
*OSPF internal



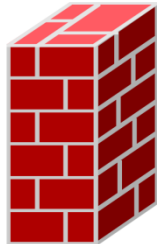
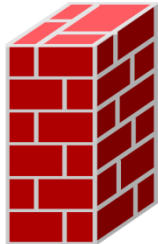
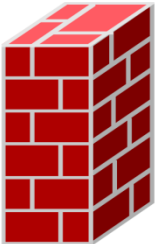
Border firewalls
ASA5580-40, 8.3(2)
*Transparent bridging



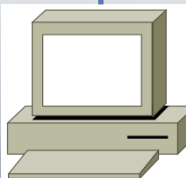
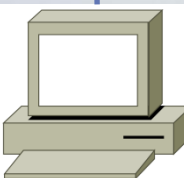
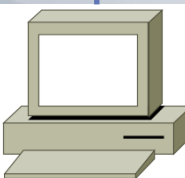
Core Routers
*OSPF



Distribution Routers
*OSPF



Unit firewalls, one per
subnet. FWSM 4.0,
multiple contexts,
*Transparent bridging



IPv4 stack

Early IPv6

- What we had to do
 - Build an addressing plan.
 - We took 32 /40s and allocated 18 to campus units, and one to allocate to existing IPv4 network owners.
 - The remaining 224 /40s are in reserve for future use.
 - Use this plan to get the ARIN assignment.
 - Get our network provider to get IPv6 to our border.
 - Route IPv6 from border to new IPv6 router and firewall.
 - Trunk unit vlans to IPv6 router.
 - IPv4 and IPv6 router or firewall interfaces do not have to be the same device

Early IPv6 network (2008)

- IPv6 router behind FWSM in routed mode
- IPv6 traffic processed in CPU, not NPU
- Limited to 500k concurrent connections
- Throughput limited to ~100Mb/s
- Different business units are behind a single policy and are not isolated from each other
- Able to provide IPv6 to early adopters that wanted it

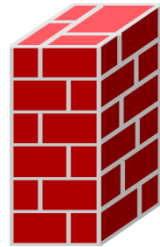
Early IPv6



Internet



Border Routers
*BGP external
*OSPF internal
*IPv6 static route



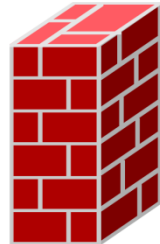
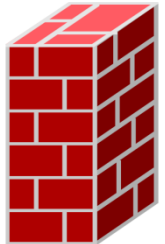
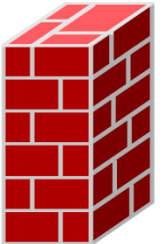
Border firewalls
ASA5580-40, 8.3(2)
*Transparent bridging



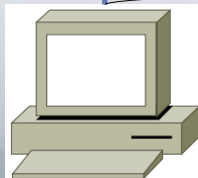
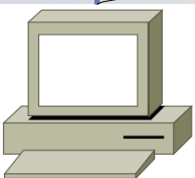
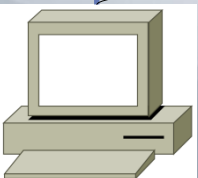
Core Routers
*OSPF



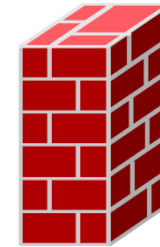
Distribution Routers
*OSPF



Unit firewalls, one per subnet. FWSM 4.0, multiple contexts, *Transparent bridging



Dual stack



IPv6 border
FWSM, routed mode
*static routes



IPv6 router
*static routes

Current IPv6 (2010)

- Replaced FWSM with context on ASA5580
 - Significantly improved performance
 - Operates in transparent mode, simplifying design
 - Security policy still shared by multiple units
 - Units still unprotected from each other
- Added IPv6 support to customer firewall management web portal

Current IPv6 (cont.)

- Departmental IPv6
 - Installed ASA5580, multiple transparent contexts
 - Will be adding unit IPv6 firewalls to operate in parallel with IPv4
 - Operating in parallel allows gradual migration to IPv6, turning it on per subnet as needed.
 - As migration continues, unit policy will move from border firewall to departmental firewalls.
 - Units will be protected from each other, mirroring our existing IPv4 model.

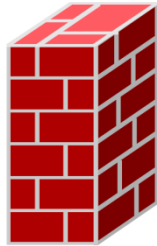
Current IPv6



Internet



Border Routers
*BGP external
*OSPF internal
*IPv6 static route



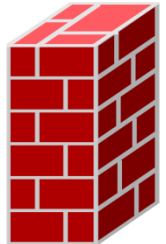
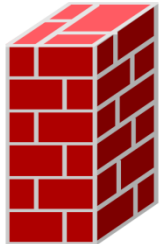
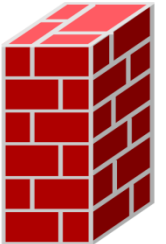
Border firewalls
ASA5580-40, 8.3(2)
*Transparent bridging



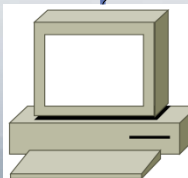
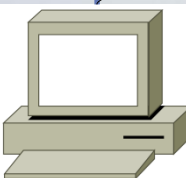
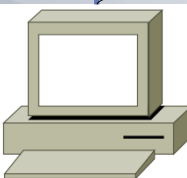
Core Routers
*OSPF



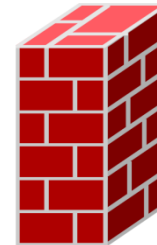
Distribution Routers
*OSPF



Unit firewalls, one per subnet. FWSM 4.0, multiple contexts, *Transparent bridging



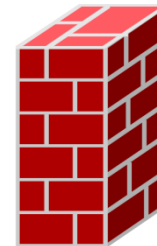
Dual stack



IPv6 border
ASA5580
*Transparent bridging



IPv6 router
*static routes



IPv6 unit firewalls.
One per subnet.
ASA5580 8.3(2)
*transparent bridging

Issues

- Limited IPv6 support in early versions of ASA8.x
 - No IPv6 transparent mode
 - No IPv6 failover
 - Both resolved with 8.2(1)
- Nested object groups not supported
 - Cisco Bug ID CSCtc71551
 - Documentation updated to reflect issue, but issue itself not yet resolved.

Example:Object-group

- IPv4-FWSM(config)# object-group network LPL
IPv4-FWSM(config-network)# network-object 192.168.1.0 255.255.255.0
IPv4-FWSM(config-network)# object-group network World-IP
IPv4-FWSM(config-network)# group-object LPL

IPv4-FWSM(config-network)# access-list Outside line 10 permit ip any object-group World-IP
IPv4-FWSM(config-network)#
- IPv6-FWSM(config)# object-group network LPL
IPv6-FWSM(config-network)# network-object 2607:F088::/56
IPv6-FWSM(config-network)# object-group network World-IP
IPv6-FWSM(config-network)# group-object LPL

IPv6-FWSM(config-network)# IPv6 access-list Outside line 10 permit ip any object-group World-IP

ERROR: IP version of object-group (IPv4) doesn't match IP version of ACL (IPv6)
- This allows creation of an object group with both IPv4 and v6 addresses that can never be used ☹.

Issues: Router Advertisements

- Router Advertisements needed for auto configuration were not passed through the firewall.
 - Cisco Bug ID CSCth46161
 - Router Solicitation was sent from host, through firewall, to Catalyst 6500
 - Router responded with RA
 - RA entered the outside interface of the firewall
 - RA packet was not passed by the firewall, no syslog message generated
 - Clients couldn't form addresses. ☹️☹️
- Resolved in version 8.3(2)1

Issues: Duplicate Address Detection

- Duplicate Address Detection (DAD) is not supported across the transparent firewall
- Cisco says this is by design because of RFC 3590
 - Use of source IP of :: is considered a spoofed packet, a security threat, and is dropped
- Potential chance that you would have identical IPs on each side of firewall.
- We're not quite sure what this means. ☹️

Issues: Management

- IPv6 management
 - Only recently can assign IPv6 management address to module, ver. 8.3
 - Cannot specify IPv6 syslog server
 - Cannot specify IPv6 tacacs server
- No full feature parity between IPv4 and IPv6. IPv4 required for proper management.
- No way to operate in a IPv6 only mode ☹️

Future IPv6

- Converged IPv4/IPv6 network and firewalls
 - Additional IPv6 hardware support on 6500s
 - Upgrade FWSMs to IPv6 capable hardware
 - Money to do the above. ☹️
- Educate campus IT staff, faculty. ☹️☹️☹️

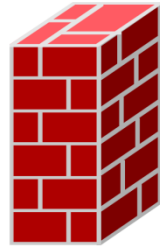
Future IPv6 Converged



Internet



Border Routers
*BGP external
*OSPF internal



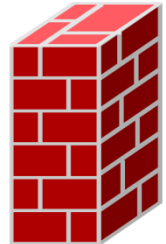
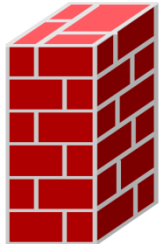
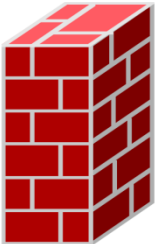
Border firewalls
ASA5580-40, 8.3(2)
*Transparent bridging



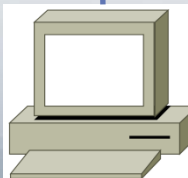
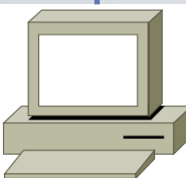
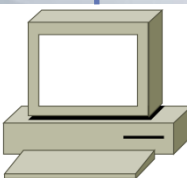
Core Routers
Dual stack
*OSPF



Distribution Routers
Dual stack
*OSPF



Unit firewalls, dual stack, multiple contexts, ASA module
*Transparent bridging



Dual stack

VPN Notes

- IPv6 enabled VPN
 - We use Cisco ASA appliances and AnyConnect VPN client, which does support IPv6
 - IPv4 customer can connect from anywhere and get assigned an IPv6 address

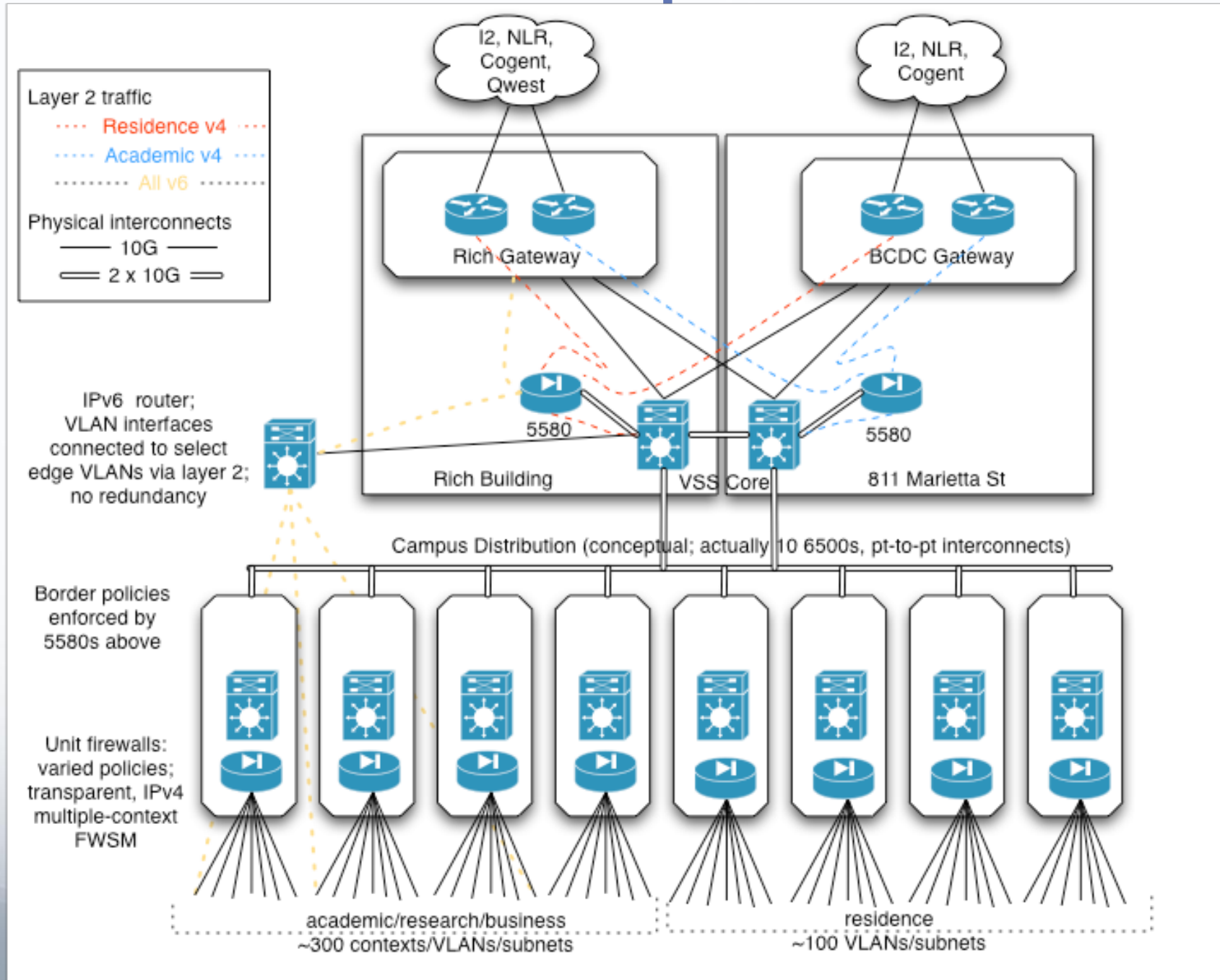
VPN Notes (cont.)

- Major problem with this is if the customer has previously installed the Cisco IPSEC VPN client on their windows machine. Installer changes MTU to 1300.
- With the MTU set to 1300, AnyConnect client will fail to connect at all if IPv6 is enabled. MTU must be reset to 1374, which may be beyond the skill of many users.
- We had this working nearly two years ago, but have not deployed to users due to potential customer support issues with MTU size.

Conclusions

- Firewall policies themselves are not dramatically different than IPv4
 - Remember that ICMPv6 must get through because Neighbor Solicitation effectively replaces ARP
 - Allow link local addresses to allow address negotiation
- Firewall performance for IPv6 is just catching up to IPv4
- Unable to manage a IPv6 only firewall at this time

Extras – Campus Network



Extras- Management App

The screenshot shows a web browser window displaying the 'OIT Firewall Setup' application. The page header includes the Georgia Institute of Technology logo and the text 'Office of Information Technology'. The main navigation bar has three tabs: 'Select Firewall', 'Firewalls', and 'Tools'. The 'Select Firewall' tab is active, showing a dropdown menu with a list of firewall names. The list includes: admin-46-fw (checked), ae-fw, alumni-fw, appliedphys-1276-fw, appliedphys-fw, arch-1901-fw, arch-85-fw, asatest-3447-fw, athletic-258-fw, athletic-449-fw, athletic-fw, audits-53-fw, bcdc-160-fw, bcdc-161-fw, bcdc-162-fw, bcdc-172-fw, bcdc-695-fw, bcdc-696-fw, bcdc-698-fw (Development), bcdc1-fw (INACTIVE), biology-66-fw, biology-71-fw, biology-88-fw, bme-434-fw, bme-439-fw, bme-448-fw, brain-1458-fw, brain-1459-fw, business-130-fw, business-41-fw, business-42-fw, business-43-fw, business-44-fw, business-63-fw, cacp-1270-fw, campus-fw, career-472-fw, cc-10-fw, cc-100-fw, cc-101-fw, cc-102-fw, and cc-103-fw. On the left side, there is a 'Current News' section with two entries: one dated 03/03/2009 and another dated 01/14/09. At the bottom left, there is a footer with the text 'main.php was last modified' and 'Copyright 2005, Georgia Institute of Technology'. On the right side, there are 'Refresh' and 'Logout' buttons. The browser's address bar and status bar are visible at the bottom.

Georgia Institute of Technology
Office of Information Technology

OIT Firewall Setup

Select Firewall | Firewalls | Tools

Please select a firewall

- admin-46-fw
- ae-fw
- alumni-fw
- appliedphys-1276-fw
- appliedphys-fw
- arch-1901-fw
- arch-85-fw
- asatest-3447-fw
- athletic-258-fw
- athletic-449-fw
- athletic-fw
- audits-53-fw
- bcdc-160-fw
- bcdc-161-fw
- bcdc-162-fw
- bcdc-172-fw
- bcdc-695-fw
- bcdc-696-fw
- bcdc-698-fw (Development)
- bcdc1-fw (INACTIVE)
- biology-66-fw
- biology-71-fw
- biology-88-fw
- bme-434-fw
- bme-439-fw
- bme-448-fw
- brain-1458-fw
- brain-1459-fw
- business-130-fw
- business-41-fw
- business-42-fw
- business-43-fw
- business-44-fw
- business-63-fw
- cacp-1270-fw
- campus-fw
- career-472-fw
- cc-10-fw
- cc-100-fw
- cc-101-fw
- cc-102-fw
- cc-103-fw

Current News:

03/03/2009:

- New page layout
- 'Folder' tabs added
- New 'action' buttons

For object groups, click on the 'more...' link. Select the object group you want to edit.

01/14/09:


- New search feature
- A new 'Firewall' audience scope is available
- The 'Firewall Listing' page now shows the IP address of each campus IP

Authorized requests are listed on the Firewall Listing and on the individual firewall pages.

main.php was last modified on 03/03/2009 at 10:00 AM
Copyright 2005, Georgia Institute of Technology

Refresh Logout

Extras – Management App2



Georgia Institute of Technology
Office of Information Technology

OIT Firewall Setup

Select Firewall

Machines List

Custom Scopes

Scheduled Uploads

test-5-175-fw.ns

This firewall is used for testing purposes only.

Subnet: 143.215.252.0/25
 Number of Servers: 128; inside VLAN 210, outside VLAN 200
 Last Edited: 2009-06-03 13:07:13
 Last Upload: 2009-04-29 23:32:19
 Authorized Requesters: Brian Flanagan (bflanagan6), Dan Forsyth (df30), Karen Carter (karenb)
 Firewall Testing:
 This is a test

Hide servers with no rules
 Show custom scope definitions
 Show firewall history

Refresh
Logout

Server	Name	Open Ports	Last Edited(Edited By)																																				
0.0.0.0/0	Firewall - Default Rules broadcast entry & 'global rule' container	<table style="width: 100%; border-collapse: collapse; font-size: x-small;"> <thead> <tr> <th style="width: 25%;">Port(s)/Protocol</th> <th style="width: 25%;">Audience</th> <th style="width: 50%;">Comment</th> </tr> </thead> <tbody> <tr><td>/esp</td><td>vpn-servers</td><td>L2TP over IPSEC</td></tr> <tr><td>/icmp</td><td>icmp-permit</td><td>icmp [default_rules]</td></tr> <tr><td>/ip</td><td>isscanners-trusted</td><td>scanners [default_rules]</td></tr> <tr><td>1-65535/tcp</td><td>nameservers</td><td>dns [default_rules]</td></tr> <tr><td>1-65535/udp</td><td>nameservers</td><td>dns [default_rules]</td></tr> <tr><td>22/tcp</td><td>123.45.67.8</td><td>Open ssh to 1 specified IP [Pre-approved rule]</td></tr> <tr><td>53/tcp</td><td>nameservers</td><td>dns [default_rules]</td></tr> <tr><td>53/udp</td><td>nameservers</td><td>dns [default_rules]</td></tr> <tr><td>113/tcp</td><td>identdallow</td><td>ident [default_rules]</td></tr> <tr><td>3489/tcp</td><td>vpn</td><td>Open 3489 to VPN [Pre-approved rule]</td></tr> <tr><td>3489/tcp</td><td>vpn</td><td>Open 3489 to VPN [Pre-approved rule]</td></tr> </tbody> </table>	Port(s)/Protocol	Audience	Comment	/esp	vpn-servers	L2TP over IPSEC	/icmp	icmp-permit	icmp [default_rules]	/ip	isscanners-trusted	scanners [default_rules]	1-65535/tcp	nameservers	dns [default_rules]	1-65535/udp	nameservers	dns [default_rules]	22/tcp	123.45.67.8	Open ssh to 1 specified IP [Pre-approved rule]	53/tcp	nameservers	dns [default_rules]	53/udp	nameservers	dns [default_rules]	113/tcp	identdallow	ident [default_rules]	3489/tcp	vpn	Open 3489 to VPN [Pre-approved rule]	3489/tcp	vpn	Open 3489 to VPN [Pre-approved rule]	2009-01-28 11:29:35 (df30)
Port(s)/Protocol	Audience	Comment																																					
/esp	vpn-servers	L2TP over IPSEC																																					
/icmp	icmp-permit	icmp [default_rules]																																					
/ip	isscanners-trusted	scanners [default_rules]																																					
1-65535/tcp	nameservers	dns [default_rules]																																					
1-65535/udp	nameservers	dns [default_rules]																																					
22/tcp	123.45.67.8	Open ssh to 1 specified IP [Pre-approved rule]																																					
53/tcp	nameservers	dns [default_rules]																																					
53/udp	nameservers	dns [default_rules]																																					
113/tcp	identdallow	ident [default_rules]																																					
3489/tcp	vpn	Open 3489 to VPN [Pre-approved rule]																																					
3489/tcp	vpn	Open 3489 to VPN [Pre-approved rule]																																					
143.215.252.1	[No DNS entry] router port		2007-08-15 22:09:20 (kb41)																																				
143.215.252.2	tsrb-cage-2960-sw.rnoc.gatech.edu	<table style="width: 100%; border-collapse: collapse; font-size: x-small;"> <thead> <tr> <th style="width: 25%;">Port(s)/Protocol</th> <th style="width: 25%;">Audience</th> <th style="width: 50%;">Comment</th> </tr> </thead> <tbody> <tr><td>20/tcp</td><td>campus</td><td>test positioning after add</td></tr> <tr><td>21/tcp</td><td>campus</td><td></td></tr> <tr><td>22/tcp</td><td>kbtest</td><td></td></tr> </tbody> </table>	Port(s)/Protocol	Audience	Comment	20/tcp	campus	test positioning after add	21/tcp	campus		22/tcp	kbtest		2009-01-27 17:52:18 (karenb)																								
Port(s)/Protocol	Audience	Comment																																					
20/tcp	campus	test positioning after add																																					
21/tcp	campus																																						
22/tcp	kbtest																																						

IPv4 – Management App3

The screenshot shows the OIT Firewall Setup web application. At the top left is the Georgia Institute of Technology logo. The main header is "OIT Firewall Setup". Below the header are navigation tabs: "Select Firewall", "Back to Machines List", and "Custom Scopes". The current page title is "test-5-175-fw.ns". On the right, there are buttons for "Back", "Help", "Refresh", and "Logout".

Server: 143.215.252.25 (zeldarose.rnoc.gatech.edu)
Last Edited: 2009-06-05 13:23:44
Scan Results:
Scan in Process

Add Pre-approved Rules
Select a rule

Show History including Removed/Expired Rules


Existing Rules for 143.215.252.25 (zeldarose.rnoc.gatech.edu)

Port(s)/Protocol	Audience	Comments	Expiration Date	Last Edited (Edited By)	Remove Rule
22/tcp	130.207.165.10			2009-05-20 14:12:20 (kb41)	<input type="button" value="Remove"/>
22/tcp	130.207.165.11	Open ssh from 1 specified IP [Pre-approved rule]	2009-10-06 00:00:00	2009-06-05 13:23:44 (bflanagan6)	<input type="button" value="Remove"/>
80/tcp	any			2009-01-15 17:40:46 (grahamt)	<input type="button" value="Remove"/>

Server Attributes for 143.215.252.25 (zeldarose.rnoc.gatech.edu)
Server Comment:

selfserv.php was last modified: May 06 2009 12:03:20.

IPv4 – Management App4


OIT Firewall Setup

Select Firewall
Machines List
Scheduled Uploads

test-5-175-fw.ns Back Refresh Logout

Uploads for test-5-175-fw.ns						
Job ID	Date Requested	Requested By	Status	Messages	Upload Started	Upload Completed
8713	2009-06-05 13:25:29	bflanagan6	Success	<pre> ===== Rule Changes ===== term width 0 pager lines 0 access-list mode manual-commit object-group network vpn no network-object 143.215.220.0 255.255.252.0 object-group service 130-207-165-11-zeldarose-rnoc-tcp tcp port-object eq ssh object-group service 130-207-165-10-tempjm-rnoc-tcp tcp port-object eq ssh object-group service 130-207-165-10-optimusprime-rnoc-tcp tcp port-object eq ssh object-group service 130-207-165-10-baskerville-rnoc-tcp tcp port-object eq 9100 object-group service 130-207-165-10-bunsen-rnoc-tcp tcp port-object eq ssh object-group service 130-207-165-10-zeldarose-rnoc-tcp tcp port-object eq ssh clear configure access-list inbound [... inbound access list suppressed ...] access-list commit access-list mode auto-commit show np 3 acl stat ===== inbound Access-list Differences ===== 45a46 > access-list inbound extended permit esp object-group vpn-servers host 143.215.252.12 50a52,54 > access-list inbound extended permit tcp host 130.207.165.10 host 143.215.252.14 object-group 130-207-165-10-tempjm-rnoc-tcp > access-list inbound extended permit tcp host 130.207.165.10 host 143.215.252.15 object-group 130-207-165-10-optimusprime-rnoc-tcp > access-list inbound extended permit tcp host 130.207.165.10 host 143.215.252.16 object-group 130-207-165-10-bunsen-rnoc-tcp 51a56,57 > access-list inbound extended permit tcp host 130.207.165.10 host 143.215.252.25 object-group 130-207-165-10-zeldarose-rnoc-tcp > access-list inbound extended permit tcp host 130.207.165.11 host 143.215.252.25 object-group 130-207-165-11-zeldarose-rnoc-tcp </pre>	2009-06-05 13:26:26	2009-06-05 13:26:55
8193	2009-04-29 21:13:55	steve	Success	<pre> ===== Rule Changes ===== </pre>	2009-04-29 23:32:06	2009-04-29 23:32:18

Extras – Management

App5

Show firewall history

Server	Name	Open Ports	Last Edited(By)																					
0.0.0.0/0 Edit SS Edit	Firewall - Default Rules Default Policy Container Copy/Link		28 Sep 2010 15:44:32 (admin)																					
IPv6 Context																								
::/0 Edit SS Edit	Firewall - Default IPv6 Rules Default Policy Container Copy From Clear all rules	<table border="0"> <tr> <td>Port(s)/Protocol</td> <td>Audience</td> <td>Comment</td> </tr> <tr> <td>1-65535/icmp6</td> <td>fe80::/10</td> <td></td> </tr> <tr> <td>1-65535/icmp6</td> <td>icmp6-permit</td> <td></td> </tr> <tr> <td colspan="3">Outbound Rules</td> </tr> <tr> <td>/ip</td> <td>ff02::/16</td> <td></td> </tr> <tr> <td>1-65535/icmp6</td> <td>fe80::/10</td> <td></td> </tr> <tr> <td>/ip</td> <td>any</td> <td></td> </tr> </table>	Port(s)/Protocol	Audience	Comment	1-65535/icmp6	fe80::/10		1-65535/icmp6	icmp6-permit		Outbound Rules			/ip	ff02::/16		1-65535/icmp6	fe80::/10		/ip	any		28 Sep 2010 15:44:32 (admin)
Port(s)/Protocol	Audience	Comment																						
1-65535/icmp6	fe80::/10																							
1-65535/icmp6	icmp6-permit																							
Outbound Rules																								
/ip	ff02::/16																							
1-65535/icmp6	fe80::/10																							
/ip	any																							
2610:148:1f00:500:223:dfff:fee0:b90 Edit SS Edit	[No DNS entry] Copy From Clear all rules	<table border="0"> <tr> <td>Port(s)/Protocol</td> <td>Audience</td> <td>Comment</td> </tr> <tr> <td>22/tcp</td> <td>campus-v6 orion.ns.gatech.edu (Steve)</td> <td></td> </tr> </table>	Port(s)/Protocol	Audience	Comment	22/tcp	campus-v6 orion.ns.gatech.edu (Steve)		27 Jan 2011 08:19:19 (steve)															
Port(s)/Protocol	Audience	Comment																						
22/tcp	campus-v6 orion.ns.gatech.edu (Steve)																							
ff00::/8 Edit SS Edit	[No DNS entry] IPv6 multicast addresses Copy/Link		28 Sep 2010 15:44:32 (admin)																					
ff02::/16 Edit SS Edit	[No DNS entry] IPv6 link-local multicast addresses Copy From Clear all rules	<table border="0"> <tr> <td>Port(s)/Protocol</td> <td>Audience</td> <td>Comment</td> </tr> <tr> <td>/ip</td> <td>fe80::/10</td> <td></td> </tr> </table>	Port(s)/Protocol	Audience	Comment	/ip	fe80::/10		28 Sep 2010 15:44:32 (admin)															
Port(s)/Protocol	Audience	Comment																						
/ip	fe80::/10																							

[Add/Remove Server](#)

Discussion

Georgia Tech Firewall Team

- Graham Thomas – graham.thomas@oit.gatech.edu
- Steve Gilbreath – steve.gilbreath@oit.gatech.edu
- Brian Flanagan – brian.flanagan@oit.gatech.edu

