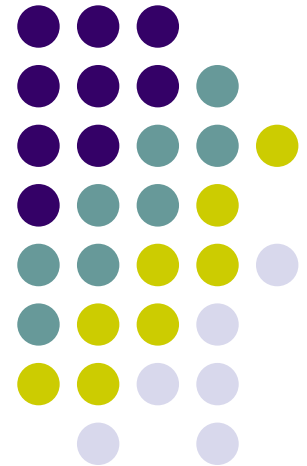


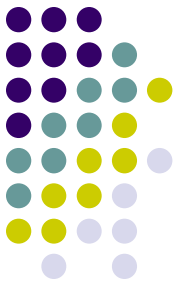
Fun With Wireless And Firewalls

Paul Asadoorian
IT Security Engineer

Don Wright
Senior Network Engineer

Brown University
August 19, 2003





Outline

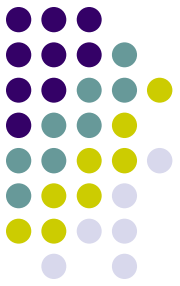
- Wireless Requirements
- Wireless: Hot or Not Technologies
- Wireless Architecture
 - Captive Portal
 - Firewalls
 - Access Points
- Wireless Challenges
- Netscreen Firewall Overview



Background

- Wireless was a requirement for Spring Semester 2003
- We set forth on the wireless path over the 2002-2003 Winter break
- It was, and continues to be, great fun!
- Many are new to Netscreen technologies

Wireless Project Requirements

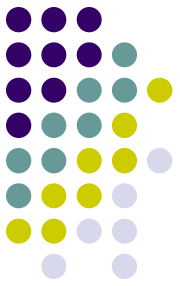


Wireless Project Requirements

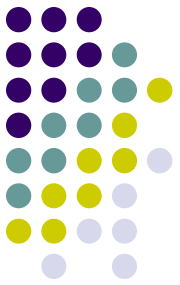


- Support wide variety of clients
 - Linux, MAC, Windows, Palm/Handheld
- Make it easy for the end user
- Security, Security, Security

Wireless Project Requirements



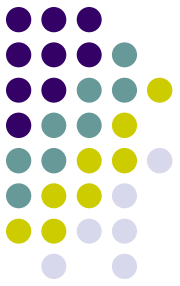
- Scalable
- Maintainable
- Integrates with our current network
- The requirement du jour



Hot or Not Technologies

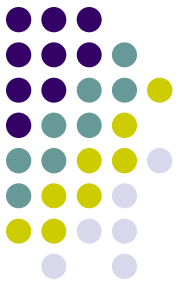
- 802.11 Alphabet Soup
- 802.1x and EAP types
 - LEAP, TTLS, PEAP...
- Captive Portals (Bluesocket, NoCat)

Hot or Not Technologies

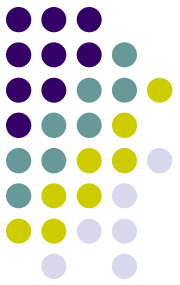


- 802.11 Alphabet Soup
 - 802.11A More expensive, didn't require throughput
 - 802.11B popular, most people have it already
 - 802.11G Not a standard at the time
 - 802.11i and WPA just not there yet

Hot or Not Technologies



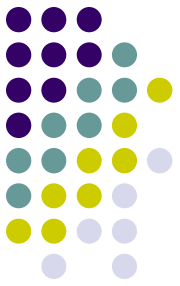
- WEP is right out



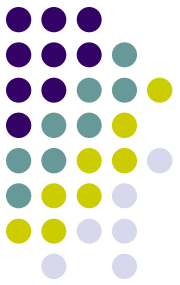
Hot or Not Technologies

- Bluesocket (Captive Portal)
 - Only validates IP and MAC address
 - Expensive
 - Has more features than we required
 - Performed well
 - Very few client problems
 - Had to reboot/restart to make changes

NoCat vs. Bluesocket



- NoCat has essentially the same functionality
- And does it *cheaply* !

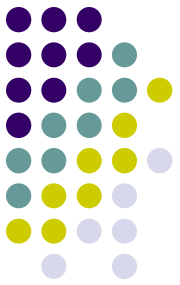


Hot or Not: Update

- Newer technologies are interesting:
 - <http://www.verniernetworks.com/>
 - <http://www.arubanetworks.com/>
 - Cisco Structured Wireless-Aware Network (SWAN)
http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_brochure09186a0080184925.html
- NoCat Specific:
 - <http://www.sputnik.com/>



Wireless Architecture



- Cisco 1100 Series Access Points
- NoCat Captive Portal Running on Linux
- Netscreen-500 Firewall

1.) Wireless client associates to an Access Point.

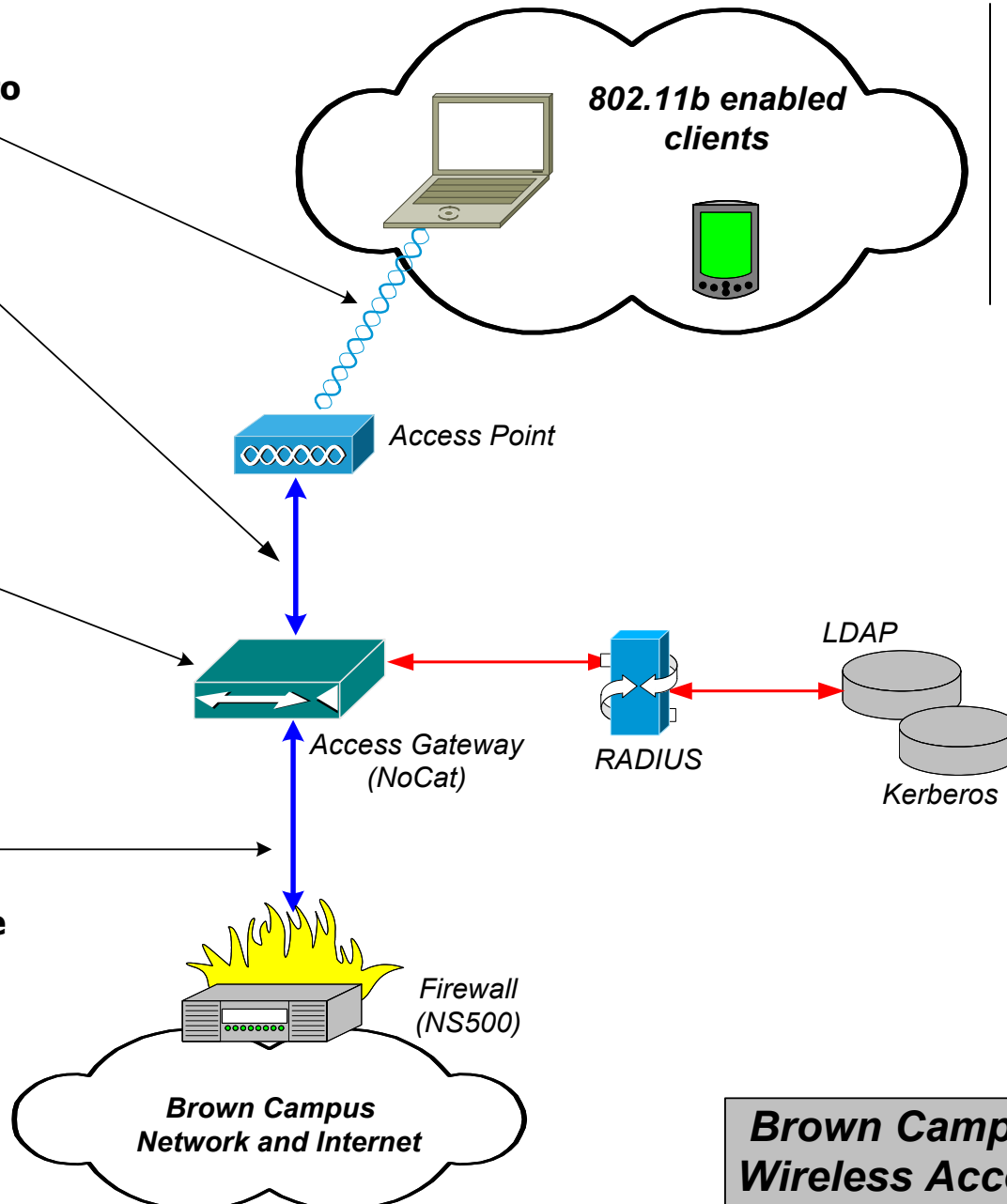
2.) Client issued a 10.x.x.x network DHCP address by Access Gateway

3.) User opens a web browser

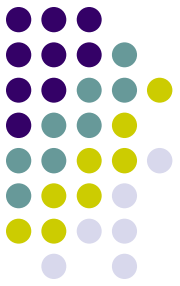
4.) Access Gateway intercepts user traffic and redirects to its login page.

5.) ShortID and password are authenticated via RADIUS to external database.

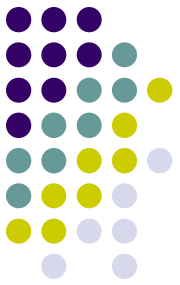
6.) Authenticated user is redirected to their browser configured home page and are now able to use the network.



Cisco Access Points



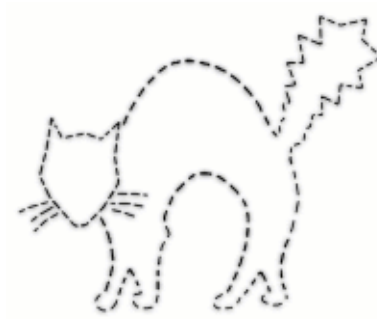
- Orinoco
- Enterasys
- We chose Cisco because....



Cisco Access Points

- 802.11b (upgradeable to 11g ~ Q403)
- Supports 802.1Q trunking
- IOS and web interface
 - PSPF (Publicly Secure Packet Forwarding)
 - Can be set from the CLI
 - TACACS+
 - SSH
 - IOS upgrades

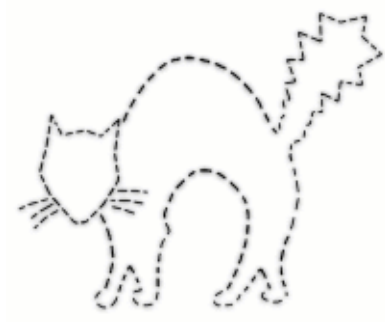
NoCat Captive Portal



Albert Einstein, when asked to describe radio, replied:

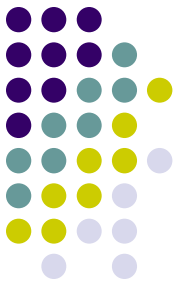
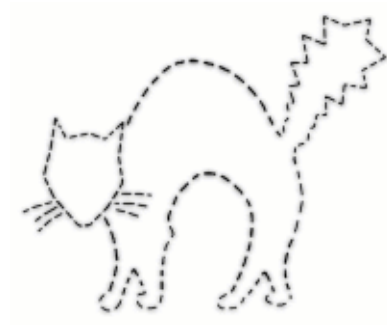
"You see, wire telegraph is a kind of a very, very long cat. You pull his tail in New York and his head is meowing in Los Angeles. Do you understand this? And radio operates exactly the same way: you send signals here, they receive them there. The only difference is that there is **no cat.**"

NoCat Captive Portal Policies



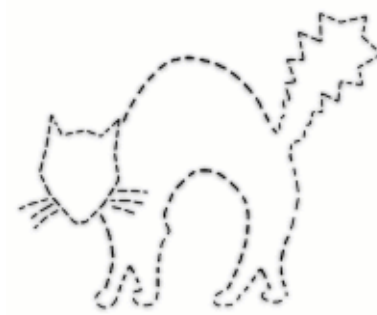
- Only allow HTTP, HTTPS, and SSH
- VPN is also allowed
- Any Brown Community member can use it

NoCat Captive Portal



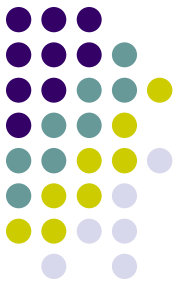
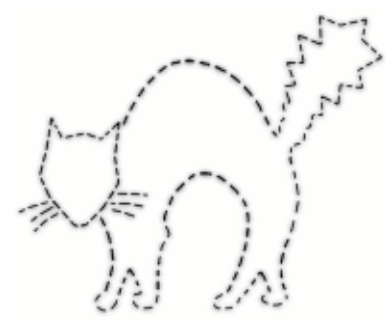
- Open Source (Free its for me!)
- Uses open and proven technologies
 - Apache, iptables, perl, Linux
- Does exactly what we need
 - Authenticate user and only allow out on certain ports

NoCat Captive Portal



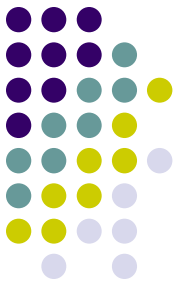
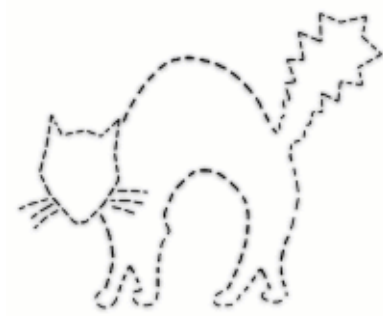
- Connects to all VLAN's using 802.1Q
- Services provided by NoCat
 - DHCP
 - HTTPS Web Server
 - RADIUS Authentication Plugin
 - iptables firewall
 - Perl script to glue it all together

NoCat Captive Portal



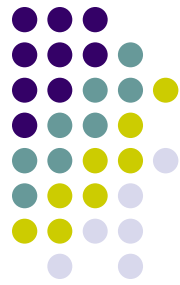
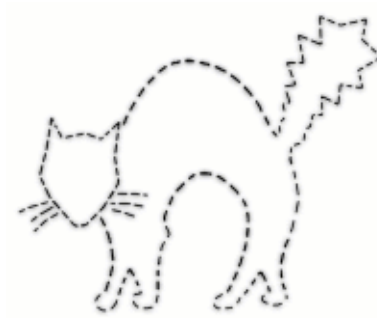
- Step 1 – DHCP address given
- Step 2 – User goes to web page
- Step 3 – NoCat intercepts and redirects them to a login page

NoCat Captive Portal



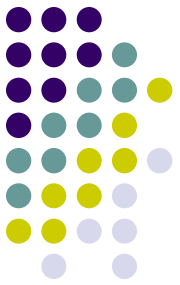
- Step 4 – User enters id and password over HTTPS
- Step 5 – User's credentials are verified
- Step 6 – If authentication is successful a firewall rule is added, and token sent to client

NoCat Captive Portal



- Step 7 – Every 10 minutes authentication is verified
 - IP address
 - MAC Address
 - Token

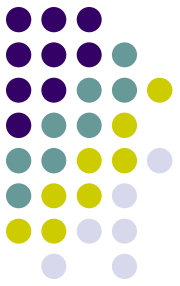
- Step 8 – A new token is issued, timer reset



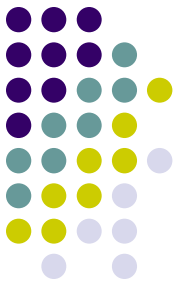
Netscreen Firewall

- Does all of the NAT
- Protects the NoCat server (Two firewalls are better than one)
- Controls where wireless users can go

Challenges – Access Points

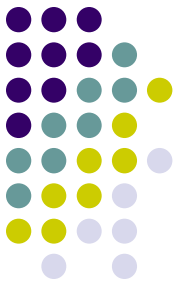


- Code not up to date
- Not all features available
- Features that sorta work



Challenges - NoCat

- Pop-up window poses problems for certain browsers
- Storing passwords in the clear
 - This problem has been fixed and will be released next week
- Usability (Login button)



Challenges - Clients

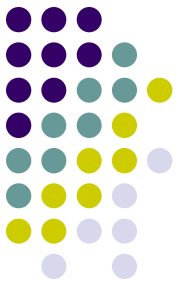
- I wrote my own web browser
- Centrino issues (MTU Sizes)
- I want to use SMTP
- Timeouts of various sorts

Netscreen



- The most common questions are usually surrounding Netscreen technologies
- Relatively new to the market
- Has many Netscreen specific terms and technologies

Netscreen



- Overview
- Terms and Concepts
- Examples
- Dos and Don'ts

Netscreen: Overview



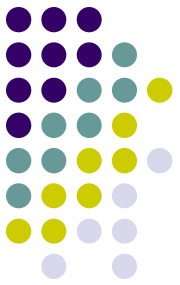
- ASIC-based hardware firewall (ScreenOS)
 - Very similar to Cisco IOS
- Very fast, stable platform
- Stateful inspection and some attack mitigation built-in
- Support for 802.1q, OSPF, and BGP

Netscreen: Overview



- Both Client and Gateway-To-Gateway VPN Support (AES-128, 3DES-128)
- Wide range of products (from 10mb/s to multi-gigabit)
- “Central Management” (Global Pro)
- Slowly replacing our Checkpoint installations

Virtual Interfaces



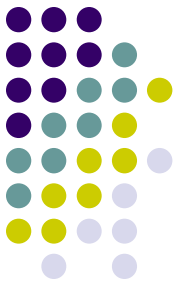
- Firewall has one physical connection
- Uses 802.1q to firewall the VLANs you assign, each called a sub-interface
- Interfaces can be placed in zones or virtual systems (Explained next)

Netscreen Concepts: Virtual Systems



- Contain one or more interfaces (Subnets)
 - Netscreen moving away from VSYS
- Allows for multiple virtual firewalls on the same device
 - Distributes administrative control
- Default Netscreen firewall device configuration features a single “root” VSYS

Netscreen Concepts: Virtual Systems



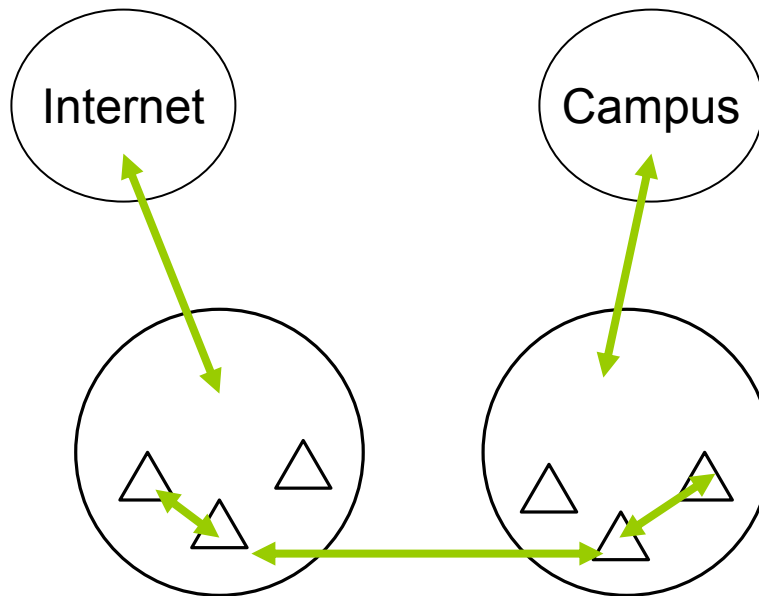
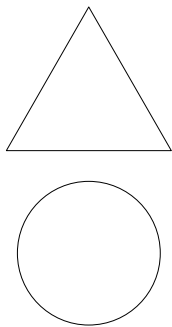
- Limitations on use of objects and groups
- Adding VSYSes splits device resources
- Can contain zones (explained later) and/or subnets

Netscreen Concepts: Zones

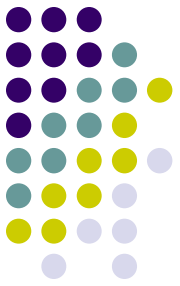


- Evolve out of operational limitations of VSYS model
- Allows for multiple virtual firewalls on the same device
 - Does not distribute administrative control
- Resources are not restricted on the same firewall
- Introduce intra-zone policy where policy can be set to manage traffic within subnets within the zone
 - Excellent for DMZ!

Zone Example



Netscreen Concepts: Virtual Routers



- Virtual Routing table
- Allows for separation of routing protocols
- Always assigned one per VSYS

Netscreen In Action



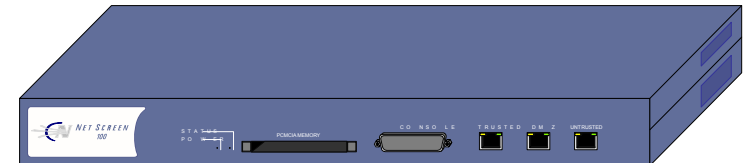
- Netscreen 5XP
- 20mb/s of throughput
- Little Firewall, Big Benefit!
 - Always keep a few extra
- Examples on campus:
 - Point-To-Point VPNs (from 10 to 100 users)
 - Single Machines
 - Entire Subnets



Netscreen In Action



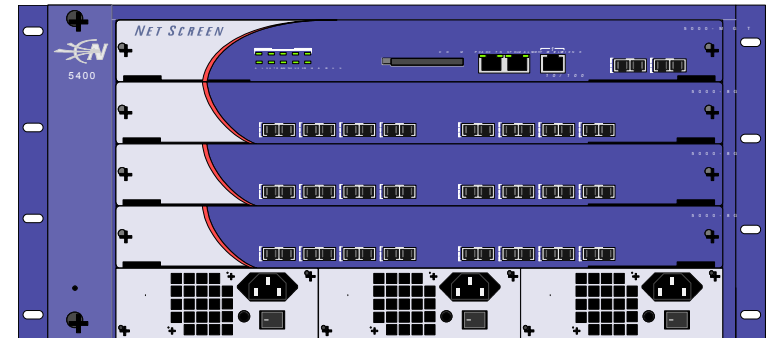
- Netscreen 25
- 100mb/s of throughput
- Examples on Campus:
 - Remote sites with 200+ users
 - Multiple VPN connections



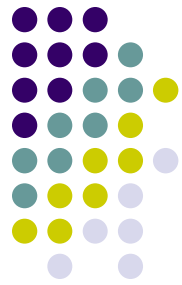
Netscreen In Action



- Netscreen 5400
- 12Gb/s of throughput
- Examples on Campus:
 - Firewall all dorms
 - Firewall all departments
 - Firewall all other workstations

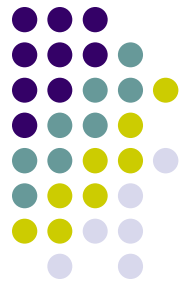


Netscreen: Dos and Don'ts

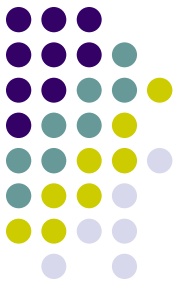


- Do use 5XP's for temporary firewalls
 - Don't forget to update the license to unlimited
- Do use Netscreen for site-site VPN
 - Don't use the Netscreen Client VPN on a large scale (Supposedly its better now)
- Do use Netscreen's attack mitigation features
 - Don't depend on them to block all attacks

Netscreen: Dos and Don'ts



- Do use the web interface for management
 - Don't use HTTP, configure a certificate and use HTTPS
- Do create your own objects and use custom timeout values
 - Don't use the default Netscreen objects
- Do use Netscreen's Web Auth feature
 - Don't allow HTTP to the web auth IP address



? Questions ?

- Paul Asadoorian
Paul_Asadoorian@brown.edu
- Don Wright
Don_Wright@brown.edu