

Security Infrastructure Overview – Part 2 Firewalls

Suresh Ramasamy
Maxis



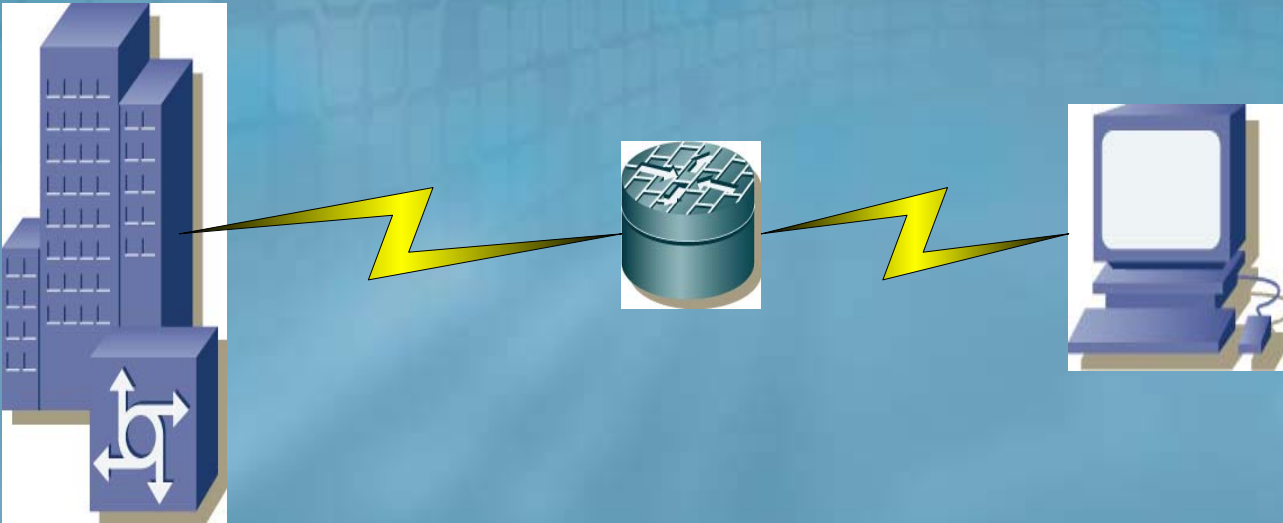
What we have covered earlier

- Overview
- Need for security infrastructure
- What is firewall
- Components of firewall
- Free firewalls (?)
- Network Design Considerations
- Summary

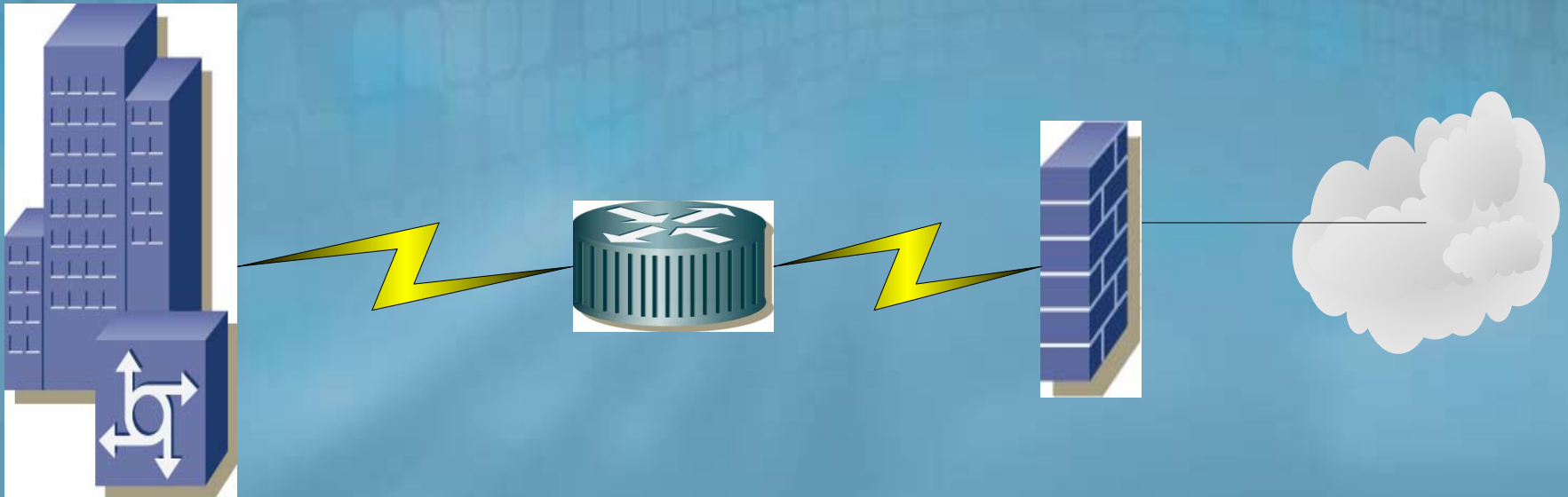
Agenda

- **Basic Network design**
- **Firewall placement**
- **Best Practices**
- **Pitfalls to avoid**
- **Additional Bonus**
- **Summary**

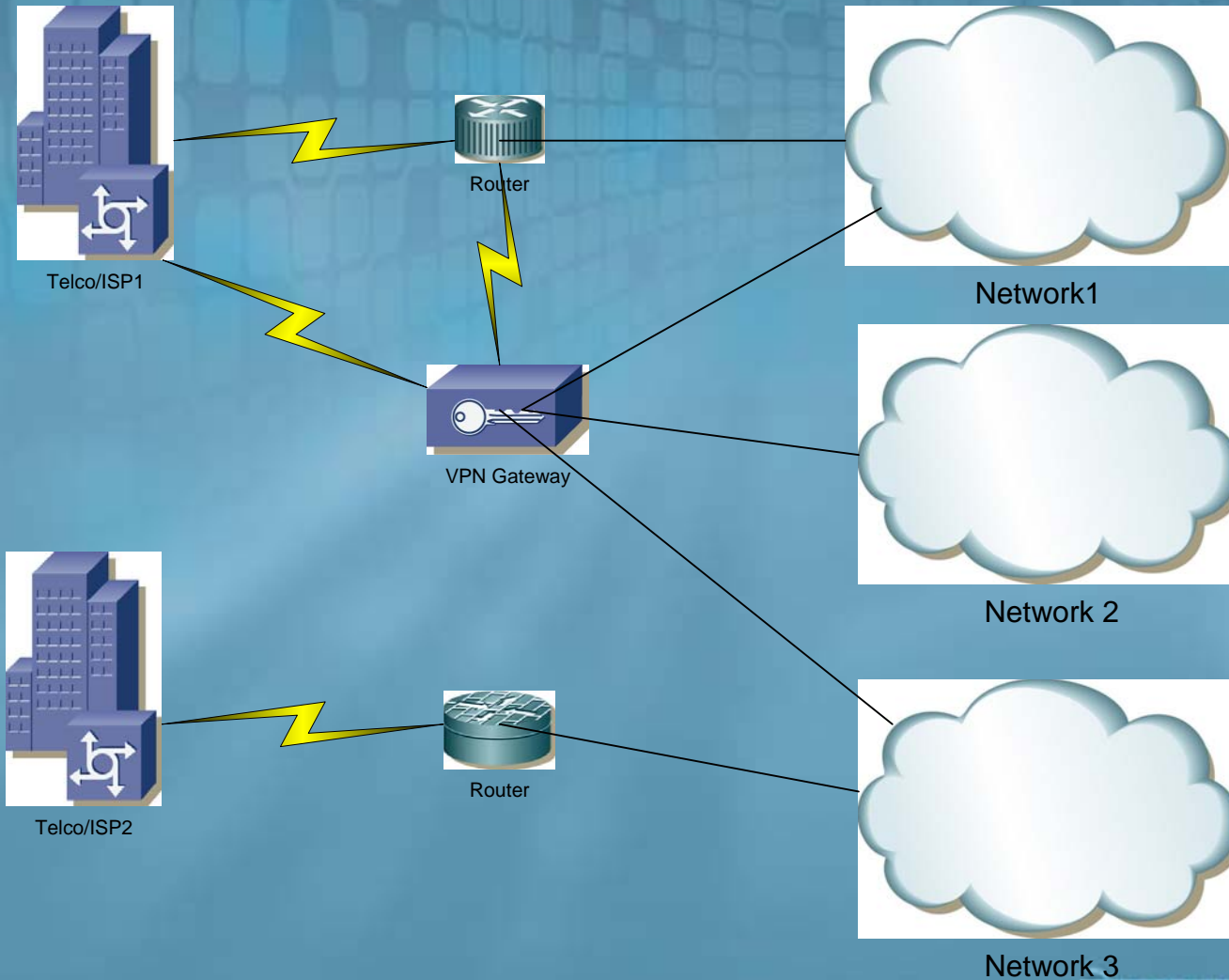
Basic Home Network



Basic Small Office/Branch Office Setup



Large Corporate Network



Golden Rule

- **Perimeter enforcement**
 - Internal v.s. External
- **Is a firewall necessary?**
 - If low load (i.e. network gateways using simple ACL, use router/switch default filtering capabilities)

Placement for Home Network

- Use filtering capabilities of ADSL router
- Linux/BSD makes the best routers around
 - Most broadband router firmware uses Linux
- NAT is still a good security option for home network

Sample of ADSL Router Filtering

The screenshot shows a Microsoft Internet Explorer browser window displaying the configuration page for a Linksys ADSL Router. The address bar shows the URL `http://192.168.1.1/policyFilters.htm`. The browser's menu bar includes File, Edit, View, Favorites, Tools, and Help. The toolbar contains icons for Back, Forward, Stop, Home, Search, Favorites, Refresh, Print, and other functions. The address bar also shows a search engine (Google) and a search box. The main content area displays the Linksys logo and a navigation menu with tabs for Filters, Forwarding, Dynamic Routing, Static Routing, DMZ Host, MAC Clone, DDNS, and Setup. The 'Filters' tab is selected, and the page title is 'LINKSYS FILTERS'. A descriptive text block explains that the Internet Filters screen allows users to block or allow specific Internet usage and set up policies for specific PCs. Below this, there is a form for configuring an Internet Access Policy. The form includes a dropdown menu for the policy name (currently '1 (-)'), 'Delete', and 'Summary' buttons. A text input field is provided for 'Enter Policy Name:'. Two radio buttons are present: 'Allow Internet Access for Listed PCs during Selected Days and Hours.' (selected) and 'Deny Internet Access for Listed PCs during Selected Days and Hours.'. The 'Days' section has checkboxes for 'Everyday', 'Sun', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', and 'Sat'. The 'Time' section has a checkbox for '24 Hours' and dropdown menus for 'From' and 'To' times (0:00 AM to 0:00 AM). An 'Edit List of PCs' button is located below the time settings. The 'Website Blocking by URL Address:' section has two text input fields. The 'Website Blocking by Keyword:' section has three text input fields. The browser's status bar at the bottom shows the URL `http://192.168.1.1/policyFilters.htm` and the connection type 'Internet'.

LINKSYS Filters Forwarding Dynamic Routing Static Routing DMZ Host MAC Clone DDNS Setup

FILTERS

The *Internet Filters* screen allows you to block or allow specific Internet usage. You can set up Internet access policies for specific PCs and set up filters by using network port numbers.

Internet Access Policy: 1 (-) Delete Summary

Enter Policy Name:

Allow Internet Access for Listed PCs during Selected Days and Hours.
 Deny Internet Access for Listed PCs during Selected Days and Hours.

Days: Everyday Sun Mon Tue Wed Thu Fri Sat

Time: 24 Hours From 0:00 AM To 0:00 AM

Website Blocking by URL Address:

Website Blocking by Keyword:

`http://192.168.1.1/policyFilters.htm` Internet

Placement for Branch Office

- Filtering to be done at the perimeter
- Depends on load, traffic
- Lesser load, use router functionality for access control
- Higher load, use firewall
- Pros and Cons based also on cost

Placement for Large Corporate

- Every entry point to be secured
- Intra network communications to be limited
- Advised using VPN site to site tunneling over public network
- Eases ACL for site to site communications
- May be complex depending on network policy/requirements

Best Practices

- **Create a security policy first**
 - Network security
 - Services security
 - Application security(Sample at SANS.org)
- **Firewall purchased in accordance to requirements**
- **Create your own requirements based on your business needs**

Pitfalls to avoid

- **Multiple layer firewall will not stop access**
- **Do not rely on firewalls as primary line of defense**
- **Avoid egg type network**
 - Hard shell
 - Soft Inside
- **Monitor your firewall**
 - Sufficient resources (CPU/Memory)
 - High Availability
 - Open Failure vs. Close Failure
 - Enable SNMP with proper ACL/community string

Lessons from the past

- **Attacks will go through firewalls**
 - **Because we open holes in it!!!!**
 - **E.g infamous PORT 80 for WEB**
- **Firewalls are PART of the security strategy, NOT THE ONLY ONE!**

Additional Bonus

- **Monitor your firewall**
- **MRTG/RRDTOOL**
 - Network Utilization
 - No of Connections
 - CPU
 - Memory
 - Firewall specific counters (refer to vendor)
- **Uses SNMP/custom perl scripts**

Resources

- Smoothwall
 - <http://www.smoothwall.com>
- MRTG
 - <http://www.mrtg.org>
- RRDTool
 - <http://people.ee.ethz.ch/~oetiker/webtools/rrdtool/>

What's next in this series?

- Virtual Private Network
 - Intrusion Detection System
 - Anti-Virus
 - Anti-Spam Solutions
 - Intrusion Prevention System
 - Correlation Tools
 - Public Key Infrastructure
-
- Provided I'm still around 😊

Questions?

- Offline : suresh@drsuresh.net