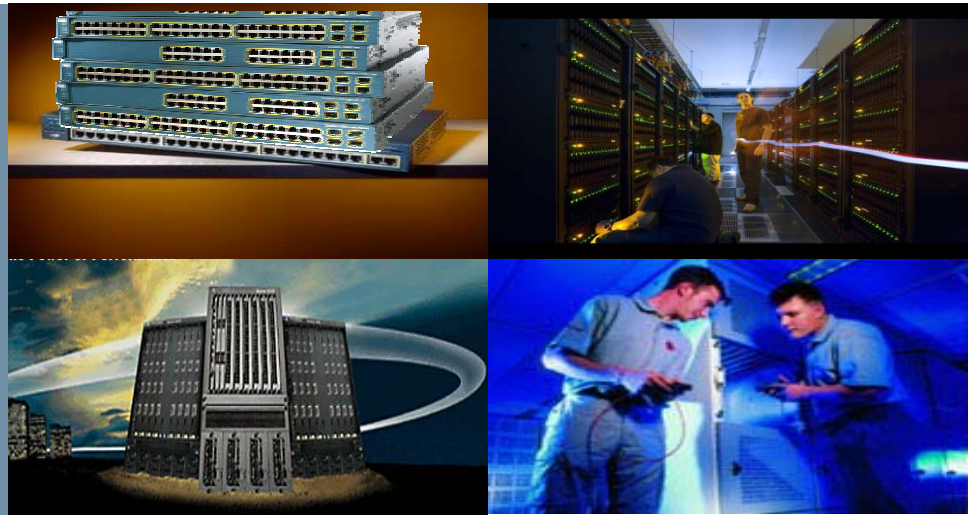
University of Mauritius

A Stateful CSG-based Distributed Firewall Architecture for Robust Distributed Security



V Ramsurrun & K M S Soyjaudah

Electrical & Electronic Engineering Dept.

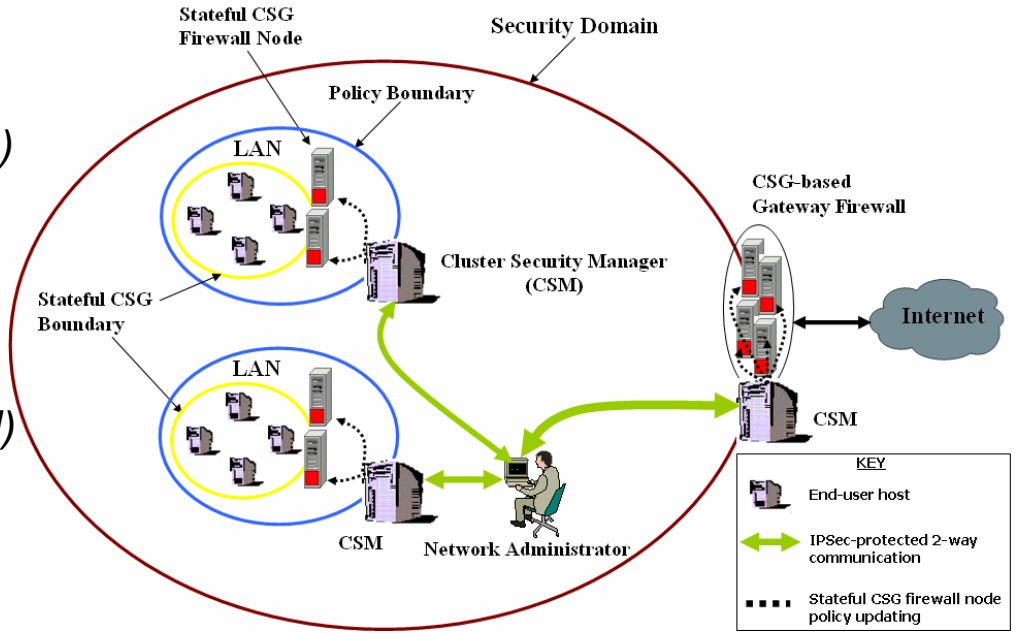
University of Mauritius

Mauritius

January 5-10, 2009

Agenda

- **Introduction**
- **Background**
  - *Distributed Firewalls*
  - *The Cluster Security Gateway (CSG) Architecture*
- **Design & Implementation**
  - *The Components*
  - *The Network Administrator Machine*
  - *The Cluster Security Manager (CSM)*
  - *The Stateful CSG*
  - *The Policy Handler*
  - *The Stateful CSG-based Gateway Firewall*
- **System Evaluation**
  - *Performance Testing*
  - *Threat Model*
  - *Qualitative Assessment*
- **Current Work**
- **Conclusion**



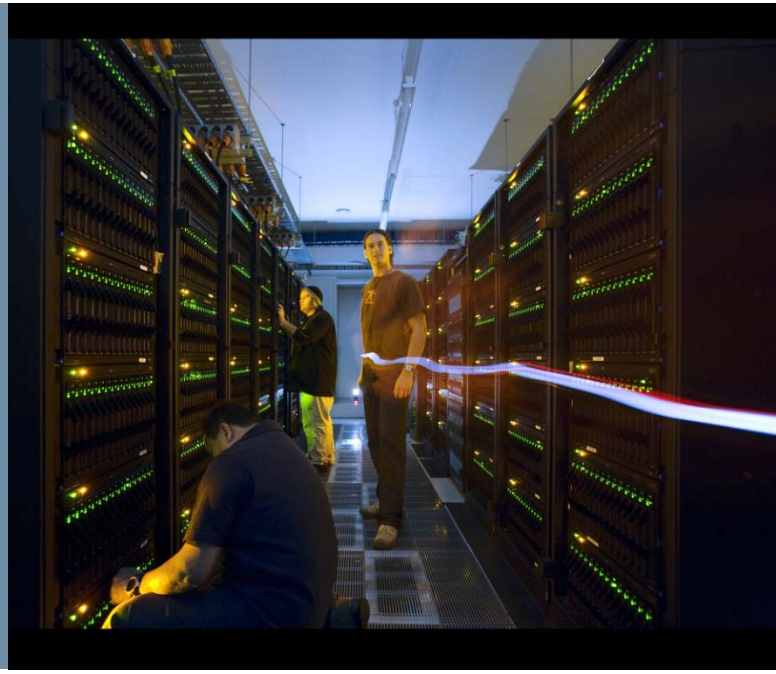
Introduction

"Every problem has in it the seeds of its own solution."
– Norman Vincent Peale

The Stateful CSG-based Distributed Firewall Architecture

- A new distributed firewall model designed primarily to address many of the limitations of distributed firewalls
- Makes use of a mix of technologies:
  - ✓ Security : L2/L3 Firewalls, Network Access Control (NAC)
    IPsec, X.509 Certificates
  - ✓ High Availability : MAC-based Load Balancing, IP Failover,
    MAC Address Takeover
- Major benefits:
  - ✓ Fine-grained security
  - ✓ Firewall tamper resistance
  - ✓ High scalability
  - ✓ Anti-spoofing
  - ✓ Anti-sniffing
  - ✓ Low overall network load
  - ✓ Secure real-time updating
  - ✓ Low convergence time
  - ✓ Low end-user host processing strain

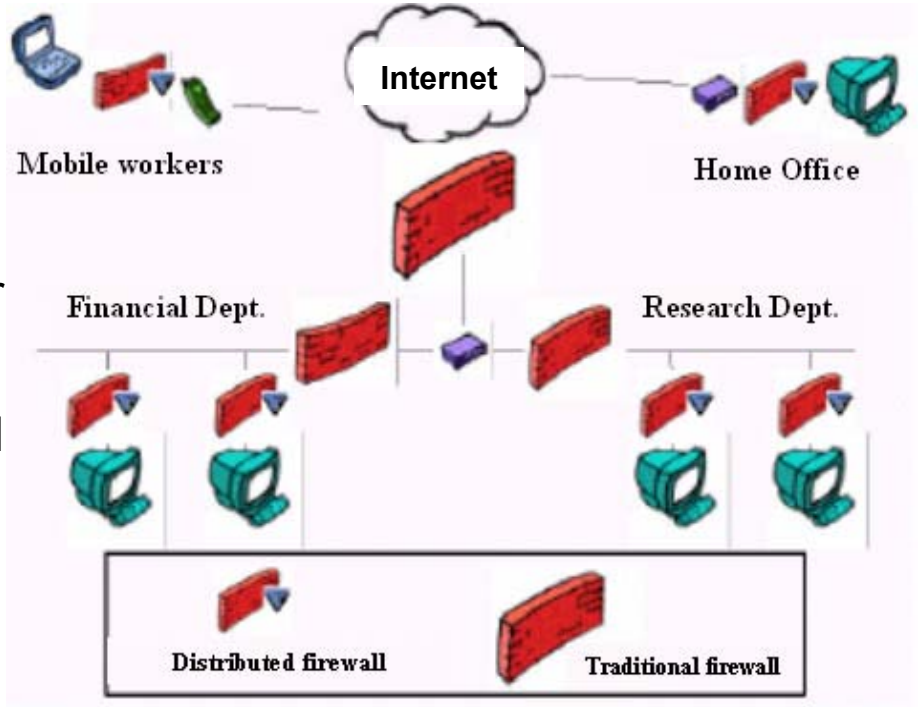
Background



"If you change the way you look at things, the things you look at change."
– Dr Wayne Dayer

Distributed Firewalls

- Pioneered by Steven Bellovin in 1999
- Created in response to the limitations of both Gateway & Host-based firewalls (more specifically, insider attacks)
- Enforces a centralised security policy but the latter is applied at the edges
- Placed at all endpoints in a network
- Conceptual design involves:
  - A general policy language for defining security policies
  - Network-wide policy distribution and application mechanisms
  - IPsec for secure policy transmission



Distributed Firewalls – Major Limitations (1)

User Tampering

- According to Wei Li, this represents the biggest problem in distributed firewalls
- Users requiring administrator privileges to work, can modify host-based firewall rules at will or completely remove the firewall, thereby exposing those hosts to attacks
- Hackers can, in turn, use those hosts as base for launching attacks from inside the network

Increase in Host Load

- There is degradation in host performance as the host-level packet filtering adds considerable load on hosts with limited resources
- In addition, with the implementation of other security tools at the host level like real-time host-based intrusion detection systems and Portsentry as in the Micro-firewall security model devised by M. Gangadharan and K. Hwang (2001), hosts will be heavily taxed

Distributed Firewalls – Major Limitations (2)

Decrease in Network Performance

- Real-time security policy updates add considerable strain on the network with all the traffic that is being generated by the distributed firewall
- As a result, the network becomes more vulnerable to DoS attacks

High Reconfiguration Time of Distributed Firewalls

- The bigger the size of a network, the more time it takes to re-deploy security policies during dynamic updating
- The convergence time of the end-user hosts and their firewalls is much higher as it is directly dependent on the number of hosts found on the network

The Cluster Security Gateway Architecture (1)

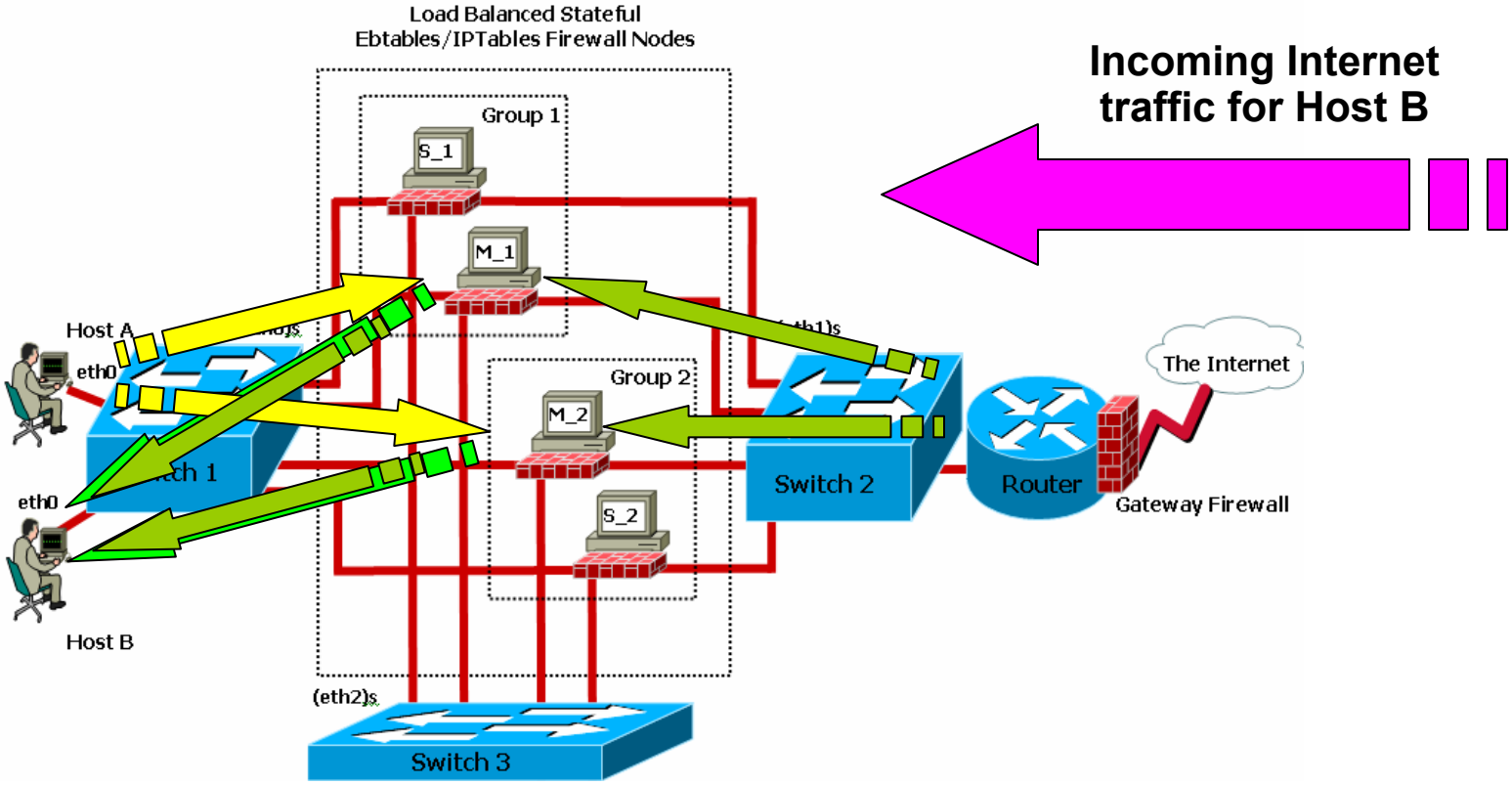
- The CSG architecture is a cluster-level security model
- It provides a methodology for grouping together multiple networking elements such as routers, security gateways, and switches in order to create more secure, more reliable switched network clusters
- Design motivation:
  - ✓If attacks are confronted at the very cluster level, distributed security will be enhanced
  - ✓Robust cluster security is far more effective than network-wide security mechanisms in reducing the occurrence of both insider & external attacks, and in limiting their spread & effects more readily

The Cluster Security Gateway Architecture (2)

- Comprises of multiple active firewall nodes working in parallel to filter traffic travelling to/from the end-user hosts of a particular cluster
  - ✓Filters intra-cluster, inter-cluster and remote communication traffic
- Uses a different type of load balancing – the Ebtables distributed sender-initiated MAC-based per-packet load balancing (PPLB) scheme
  - ✓Load balancing is done by the end-user nodes themselves
  - ✓A Layer 2 PPLB scheme developed primarily for a seamless integration in load balancing setups involving stealth firewalls
  - ✓Load balances network traffic onto MAC addresses rather than IP addresses
  - ✓Can be successfully utilized in IP-based networks as well
  - ✓Prevents the creation of single points of failure by removing the need for a dedicated load balancer
  - ✓Integrates well in already-in-place switched networks so that no major network re-design is required

The Cluster Security Gateway Architecture (3)

- A 2-active-node stateful CSG for securing one particular cluster
- Uses a modified Conntrackd codebase for ***firewall state synchronization***
- Uses Keepalived for ***failover***
- Uses GNU Mac Changer for ***MAC address takeover***



The Cluster Security Gateway Architecture (4)

- Preliminary intra-cluster performance testing using Iperf TCP sessions highlighted the following trends:
  - ✓The processing load on the end-user nodes decreases greatly
  - ✓The packet filtering strain on the firewall nodes is relatively evenly distributed
  - ✓With the load balancing scheme, the throughput is improved significantly

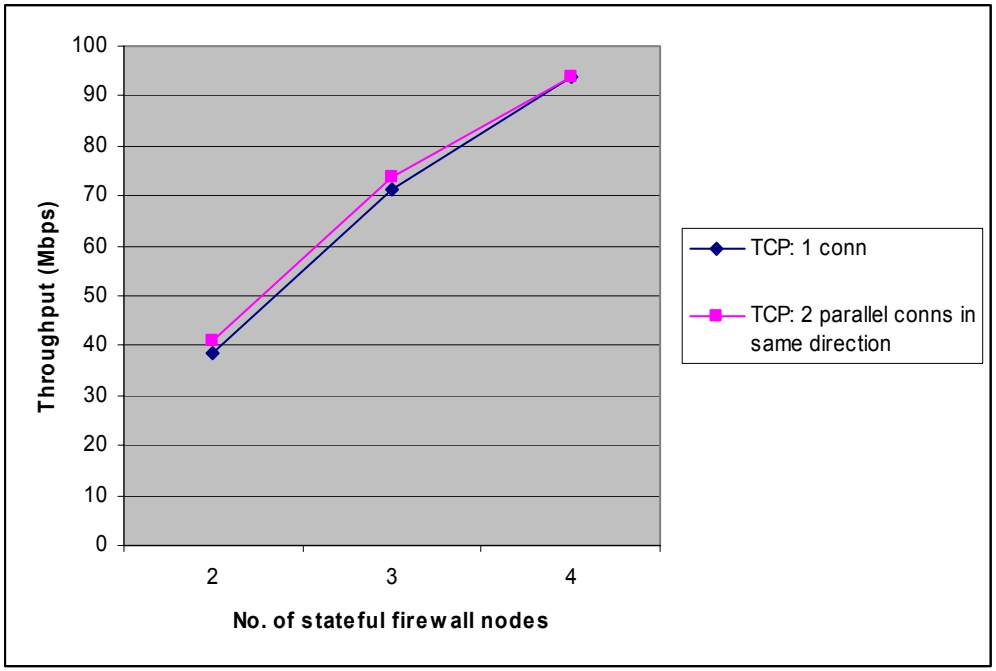


Figure 1: Variation of the throughput achieved v/s the no. of firewall nodes with a 1000-rule stateful IPTables firewall

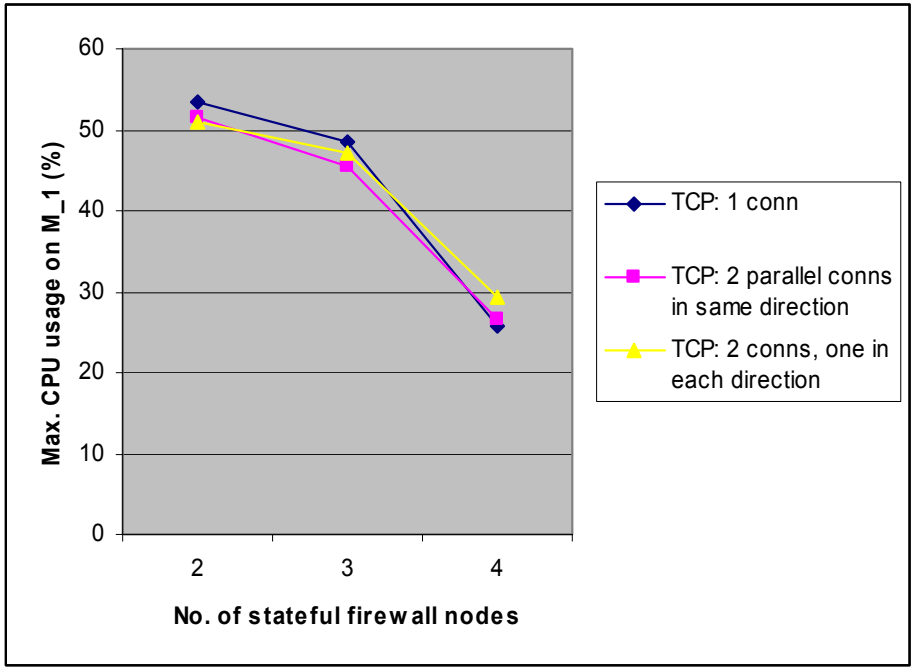


Figure 2: Variation of the maximum CPU usage recorded on firewall node M_1 v/s the no. of firewall nodes with a 1000-rule stateful IPTables firewall

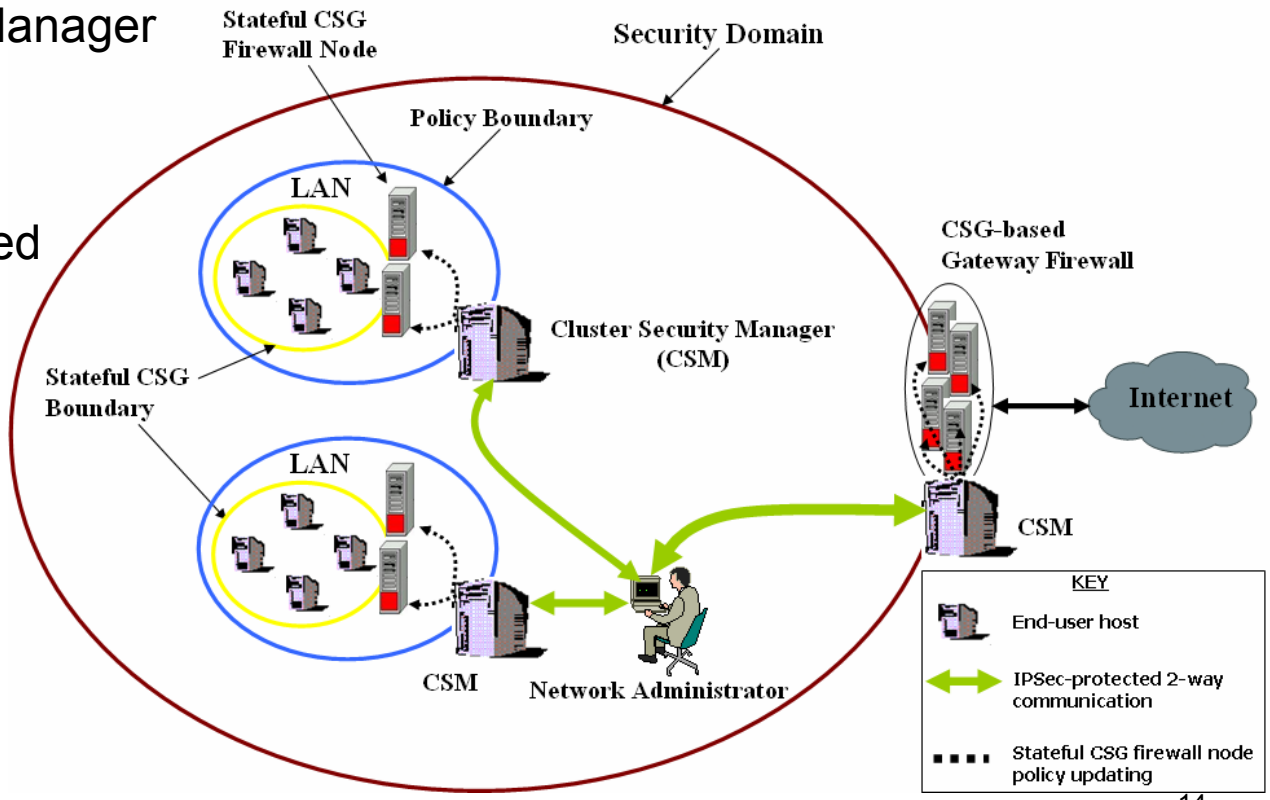
Design & Implementation

"An idea that is developed and put into action is more important than an idea that exists only as an idea."

– Buddha

The Components

- The CSG distributed security architecture is made up of several components:
  - ✓The Network Administrator Machine
    - *The Policy Repository*
    - *The Policy Distributor*
  - ✓The Cluster Security Manager
  - ✓The Stateful CSG
    - *The Policy Handler*
  - ✓The Stateful CSG-based Gateway Firewall



The Network Administrator Machine

- Is used by the Network Administrator for managing the various network and security components
  - ✓ It is from this computer that the Network Administrator updates CSG firewall nodes
  - ✓ Contains two major components – the *Policy Repository* and the *Policy Distributor*.

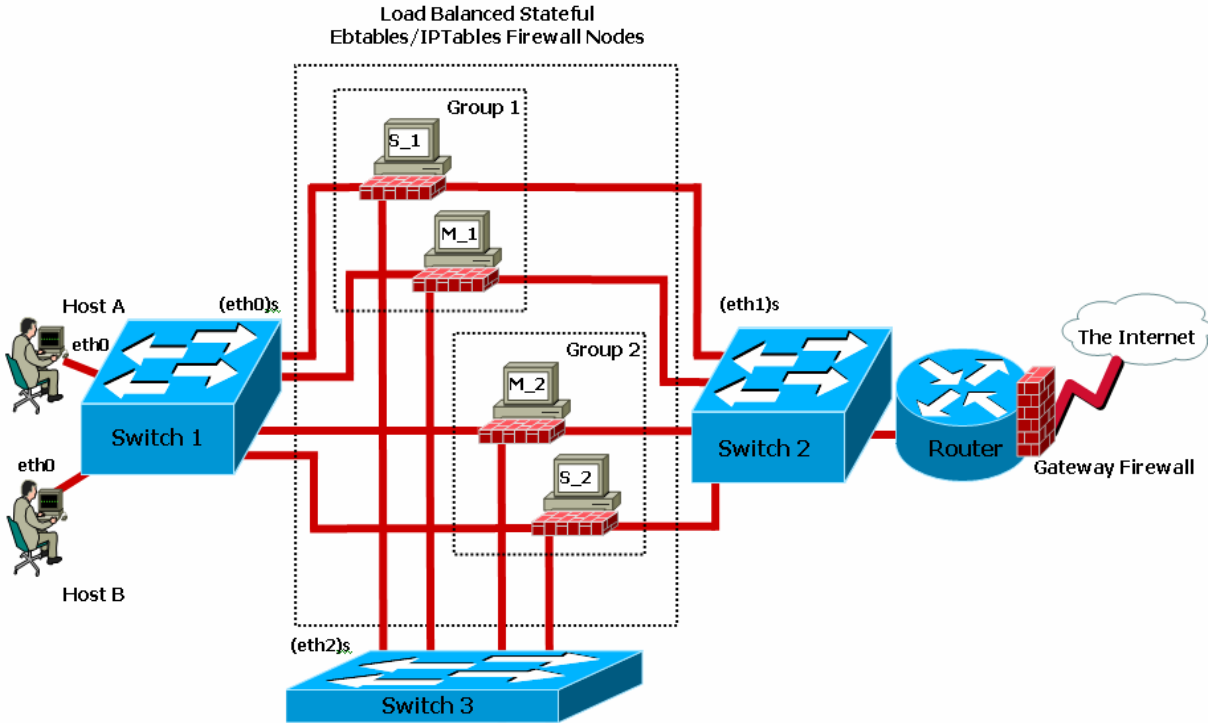
- The Policy Repository
  - ✓ Is a ***central database*** where all firewall scripts deployed in the network and all firewall updates are stored
  - ✓ Used by the Network Administrator to consult existing firewall scripts in order to create new firewall update files when the network is under attack
  - ✓ The firewall scripts and update files are stored in usable forms (for example, as *.sh* files) for direct application onto the firewall nodes
  - ✓ File versioning and creation details are also kept
- The Policy Distributor
  - ✓ Used by the Network Administrator for ***sending firewall updates*** to Cluster Security Managers (CSMs)
  - ✓ Establishes ***authenticated & encrypted end-to-end connections*** with the appropriate CSMs for secure firewall update transmission across network (IPsec + X.509 certificates)
  - ✓ ***Unicast transmission mode*** is preferred over multicast as not all the CSMs will need updating at a particular point in time, thus preventing their respective rulesets to increase in size unnecessarily

The Cluster Security Manager (CSM)

- Is the first and foremost recipient of firewall updates from the Policy Distributor
  - ✓Is the endpoint of the secure connections established by the Policy Distributor
  - ✓Consists of a user-level process that receives and distributes firewall updates to the CSG firewall nodes falling under its responsibility
  - ✓Direct updating of CSG firewall nodes is not done as the latter will act as IPsec gateways, thus considerably reducing their efficiency and throughput
  - ✓The CSM establishes unicast TCP connections to the CSG firewall nodes by reading their IP addresses from a file, *fw_list.txt,* created by the Network Administrator on the CSM
  - ✓Notifies the Network Administrator of any firewall update distribution failure
- Each end-user cluster has exactly one CSM

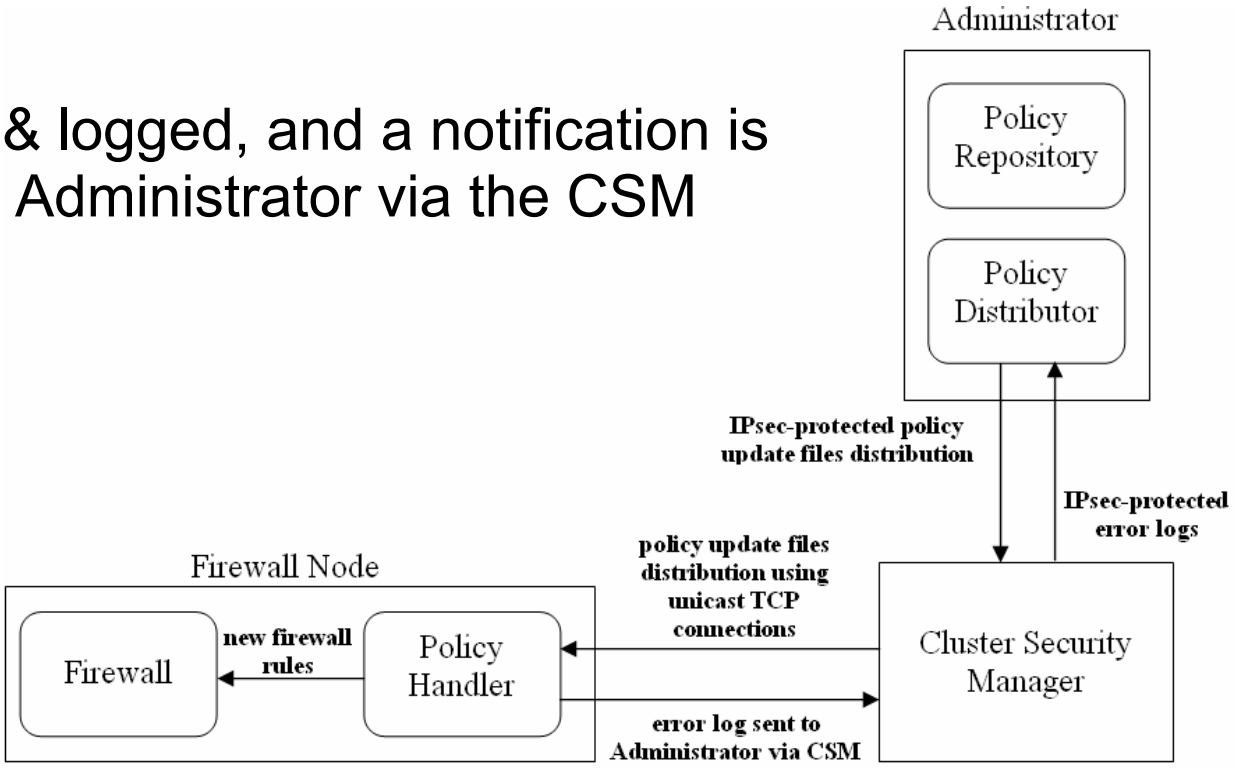
The Stateful CSG

- A 2-active-node stateful CSG for securing one particular cluster
  - ✓Two master (active) firewall nodes and two standby (backup) firewall nodes
  - ✓Layer 2 and Layer 3 packet filtering using Ebtables and IPTables respectively
  - ✓Network Access Control (NAC) is provided by applying switch MAC ACLs on specific switch ports to ensure that end-user hosts communicate only via the firewall nodes
  - ✓Port security is used to prevent source MAC address spoofing



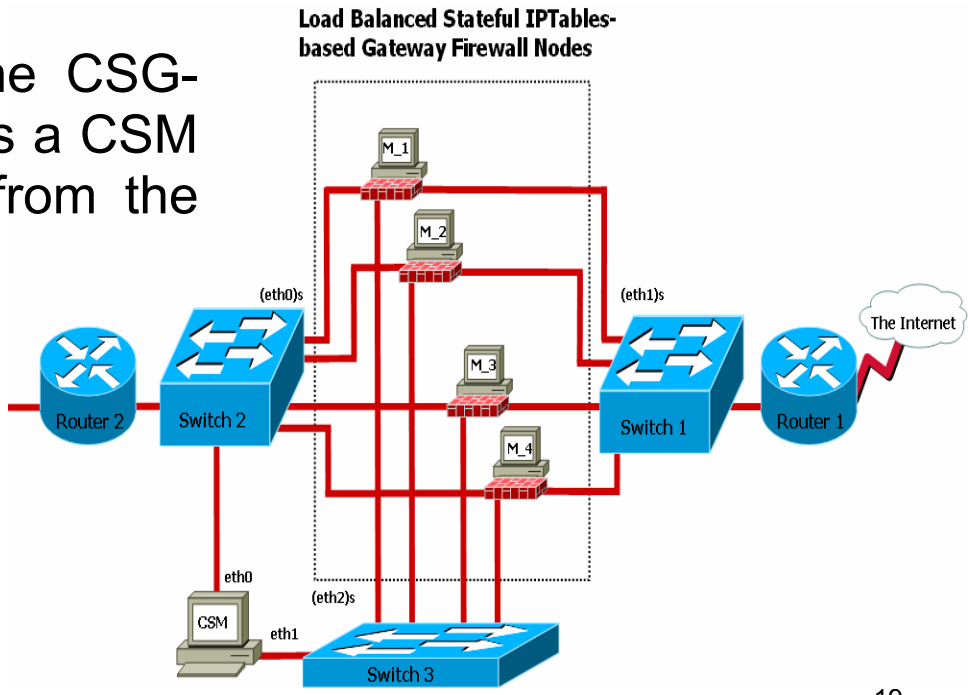
The Policy Handler

- Runs on each of the firewall nodes as a user-space TCP application
- It receives updates from its CSM and integrates them in the current firewall ruleset
  - ✓Since updates are in directly usable format, firewall rules can be inserted or deleted easily
- Any error is caught & logged, and a notification is sent to the Network Administrator via the CSM

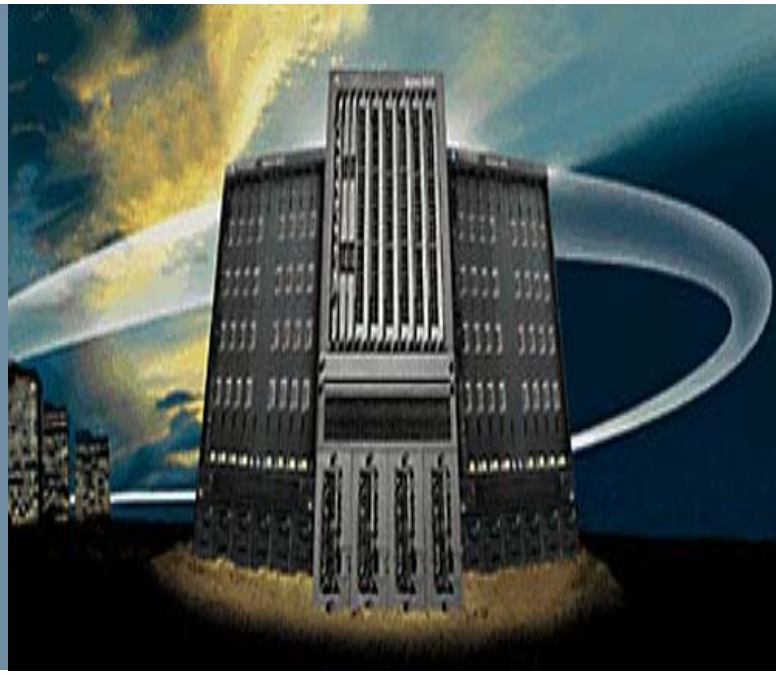


The Stateful CSG-based Gateway Firewall

- In our security model, a CSG-based gateway firewall is used
  - ✓The gateway firewall, which is the first line of access control & protection against external attacks, needs dynamic updating as well in the face of emerging threats
  - ✓Load balancing and failover techniques not only help in eliminating the single point of failure, but also help boost gateway firewall throughput and reliability
  - ✓Like the end-user clusters, the CSG-based gateway firewall, too, has a CSM for receiving firewall updates from the Network Administrator



System Evaluation



"If you have built castles in the air, your work need not be lost; that is where they should be. Now put the foundations under them."
– Henry David Thoreau

Performance Testing

- Iperf and Netio have been used to provide some throughput estimates of the secure connections between the Network Administrator machine and a CSM
- The results obtained with Iperf and Netio respectively for different IPsec transforms are as follows:

Table 1: Performance results from Iperf for different IPsec transforms

Transform	Bandwidth (Mb/s)
w/o IPsec	94.1
3DES & MD5	46.7
DES & MD5	89.8
3DES & SHA1	35.4

Table 2: Performance Results from Netio for Different IPsec Transforms

Packet size	Bandwidth w/o IPsec (KB/s)	Bandwidth with IPsec (KB/s)		
		3DES & MD5	DES & MD5	3DES & SHA1
1KB	11474	5767	10386	4159
2KB	11511	5803	10588	4465
4KB	11512	5835	10918	4466
8KB	11511	5854	10991	4485
16KB	11507	5848	10983	4471
32KB	11508	5812	10861	4457

Threat Model (1)

- The system has been assessed qualitatively against various insider and external threats

Insider Attacks

- Insider attacks come in 2 flavours – intra-cluster & inter-cluster
- Each CSG has ***cluster-specific firewall rules*** defined for both ingress and egress packet filtering in addition to the general network-wide security policy
- Intra-cluster attacks are prevented by ***switch MAC ACLs*** that do not allow direct communication between end-users
- Inter-cluster attacks are prevented by ***successive packet filtering***, performed once by the CSG of each of the clusters involved in the communication

Threat Model (2)

IP & MAC Address Spoofing

- ***Port security***, an in-built security mechanism provided by the 2970 series Catalyst switch, prevents ***source MAC address spoofing*** of outgoing end-user host packets
- Ebtables packet filtering rules using the ***--among-src match***, which allows several MAC/IP source address pairs to be defined and against which packet headers are checked, help prevent ***IP address spoofing***

Denial of Service

- Not all types of DoS attacks can be handled by distributed firewalls. DoS attacks, which rely on IP spoofing mechanisms, can be handled quite well since IP spoofing is difficult to realize within the CSG architecture
- Use of load balancing techniques in the CSG spreads the packet filtering strain over multiple firewall nodes and prevents the latter nodes from quickly becoming chokepoints

Threat Model (3)

Packet Sniffing

- ***Switch MAC ACLs*** help restrict multicast/broadcast traffic on a cluster, thus significantly decreasing traffic on the switch that attackers can sniff
- The switch makes use of ***virtual circuits***, which prevents sniffing of unicast traffic of other end-user nodes

Rule Tampering

- The filtering rules are not found on the end-user nodes, but rather on ***dedicated CSG firewall nodes***
- The maximum an un-cooperating “insider” can do is change the load balancing rule

Qualitative Assessment (1)

- The new distributed security model has been compared with other well-known distributed firewall models in terms of the advantages and characteristics they exhibit
- Distributed firewall models studied:

Table 3: The Major Distributed Firewall Schemes That Were Studied

Distributed Firewall Model	Implementation type	Developed by	Year
STRONGMAN	Software	Keromytis et al.	2003
Smokey	Software	R. Rubin	2002
The Micro-firewall Approach	Software	M. Gangadharan & K. Hwang	2001
Embedded Firewall (EFW)	Hardware	T. Markham & C. Payne	2001
Autonomic Distributed Firewall (ADF)	Hardware	Adventium Labs	2001
Network Edge Security (NES)	Hardware	T. Markham & C. Payne	2001

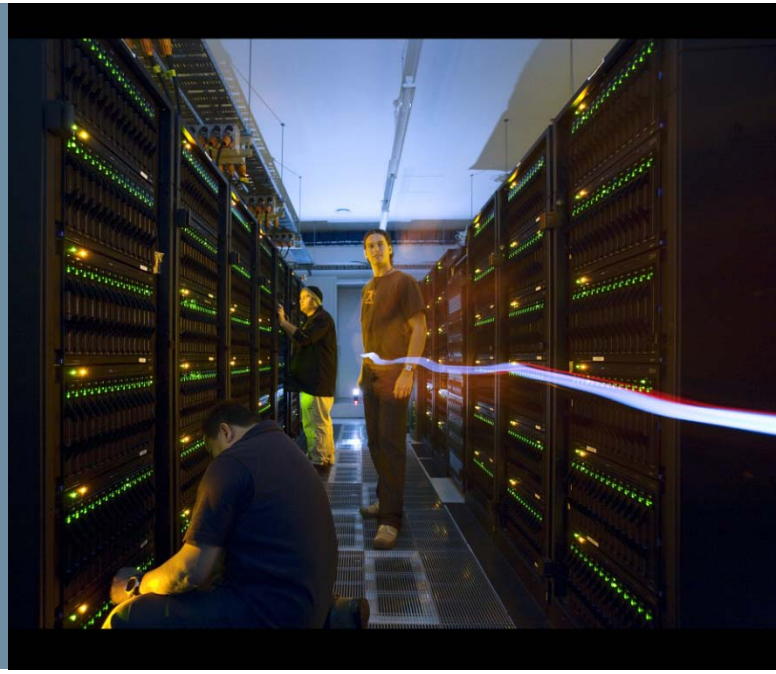
Qualitative Assessment (2)

Table 3: Comparison of the Stateful CSG-based Distributed Firewall with other Major Distributed Firewall Schemes

Characteristics	Strongman	Smokey	M-F	EFW	ADF	NES	CSG
Fine-grained security	✓	✓	✓	×	×	×	✓
Firewall tamper resistance	×	×	×	✓	✓	✓	✓
High scalability	✓	✓	✓	✓	✓	✓	✓
Anti-spoofing	✓	✓	✓	✓	✓	✓	✓
Anti-sniffing	×	×	×	✓	✓	✓	✓
Low overall network load	×	×	×	×	×	×	✓
Secure real-time updating	✓	×	✓	✓	✓	✓	✓
Low convergence time	×	×	×	×	×	×	✓
Low end-user host processing strain	×	×	×	✓	✓	✓	✓
Transparency	×	×	×	×	×	×	✓
Context knowledge	✓	✓	✓	×	×	×	×

KEY: M-F = Micro-firewalls
EFW = Distributed Embedded Firewall
ADF = Autonomic Distributed Firewall
NES = Network Edge Security

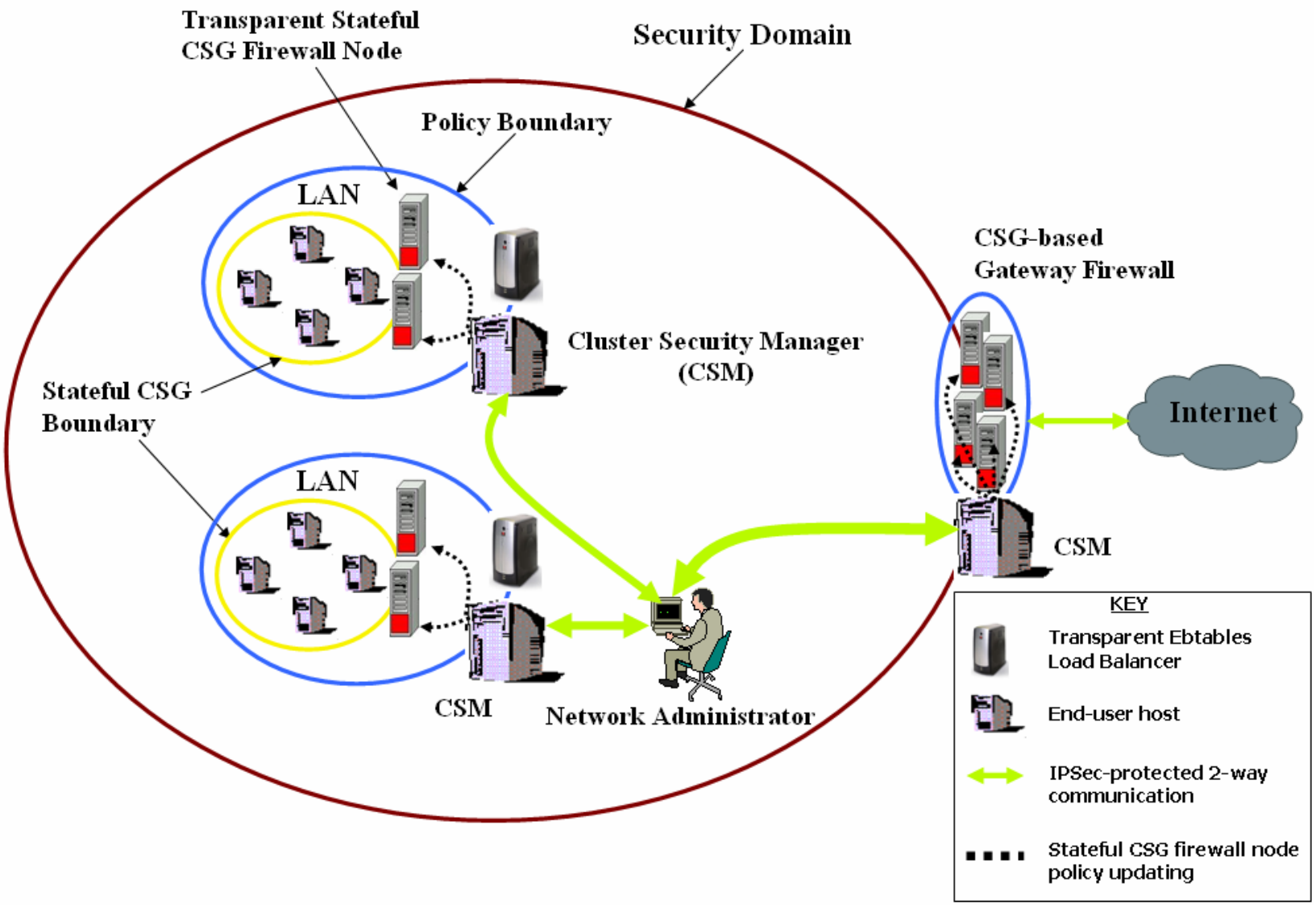
Current Work



"There is only one way in which a person acquires a new idea; by combination or association of two or more ideas he already has into a new juxtaposition in such a manner as to discover a relationship among them of which he was not previously aware."

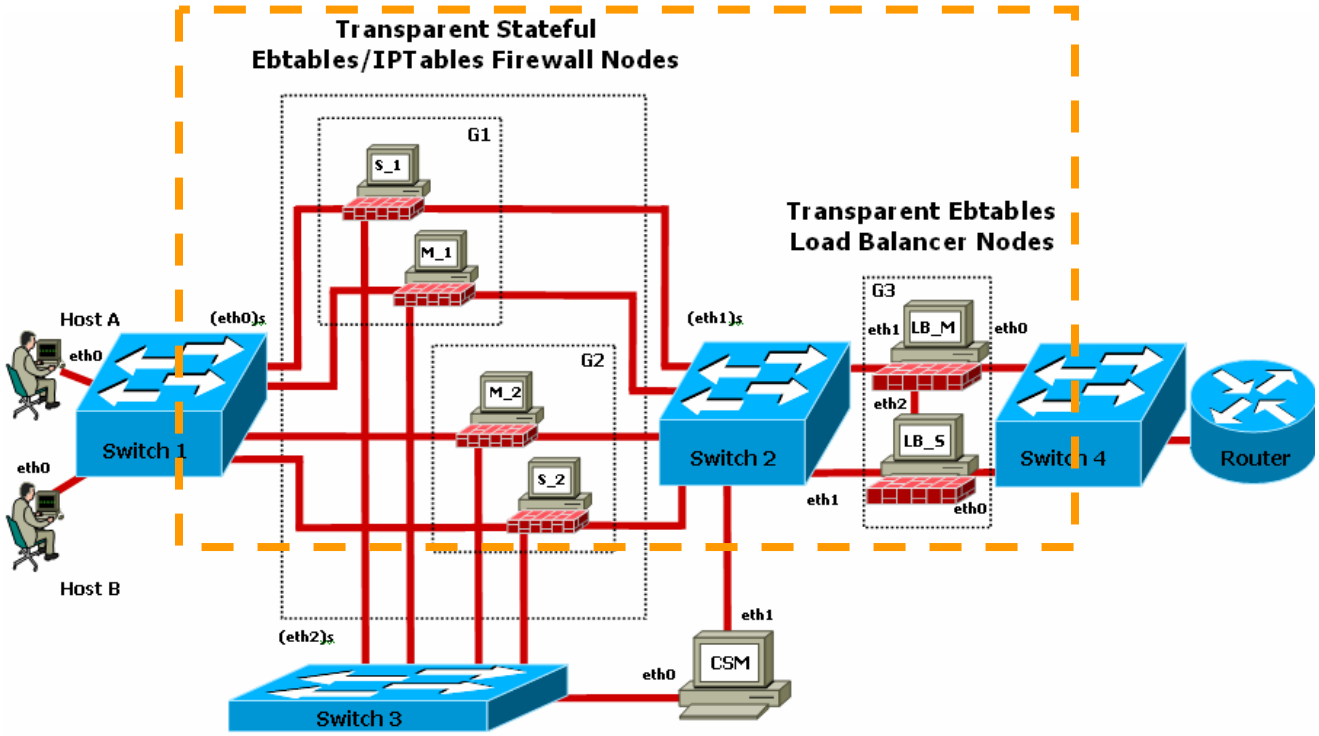
– Francis A. Carter

The Transparent Stateful CSG-based Distributed Firewall Architecture



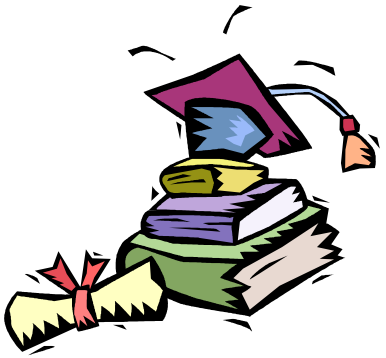
The Transparent Stateful CSG Architecture

- The whole security high-availability setup (CSG + Ebtables load balancer) is made Layer-3-transparent
  - ✓No IP addresses are used along the communication traffic travel path
- Transparency ensures greater security
  - ✓Makes the security system more difficult to locate and attack
  - ✓Helps restrict attacks to Layer 2



Future Work

- Creation of load balancing network interface cards (LB-NICs)
  - ✓Involves the incorporation of the Ebtables MAC-based load balancing scheme onto a tamper-resistant network interface card with on-board processing engines
  - ✓This approach adopts a similar line of thought as that used in the implementation of hardware-based distributed firewalls like EFW and ADF
  - ✓These load balancing cards will have to register with a central policy server first in order to be able to function
  - ✓The central policy server will perform LB-NIC group management, where each LB-NIC group will consist of all the end-user node NICs forming part of a particular end-user cluster
- Potential advantages:
  - ✓Load balancing rule tamper resistance
  - ✓Easier addition/removal of firewall nodes in the CSG
  - ✓No need for a dedicated load balancer



Conclusion

"Not every end is the goal. The end of a melody is not its goal, and yet if a melody has not reached its end, it has not reached its goal."

– Friedrich Nietzsche

Key Contributions (1)

- We have presented the stateful CSG-based distributed firewall model
- Provides for robust distributed cluster and network security
- Addresses many of the limitations of distributed firewalls
  - ✓ Firewall rule tamper resistance
  - ✓ Improved end-user host performance
  - ✓ Better overall network performance
  - ✓ Low firewall convergence times
- Provides other advantages:
  - ✓ Anti-spoofing, anti-sniffing, high scalability, secure real-time protection…

Key Contributions (2)

- Analysis of several software-based and hardware-based distributed firewalling systems
- Development of the stateful CSG-based gateway firewall for providing highly available front-line defense mechanisms
- Development of the stateful CSG-based distributed firewall architecture for robust distributed cluster-level and network security
- Development of the transparent stateful CSG-based distributed firewall architecture

Thank you for your attention ! ☺

QUESTIONS ??