

Lockdown:

Distributed Policy Analysis and Enforcement within the Enterprise Network



Problem: Managing, deploying, enforcing, and verifying security policy within an enterprise network.

Solution: By using a system of collection agents, data mining, visualization, and Linux Security Modules (LSM) Lockdown is able to achieve efficient policy creation, enforcement, and verification based upon the local context of a host.

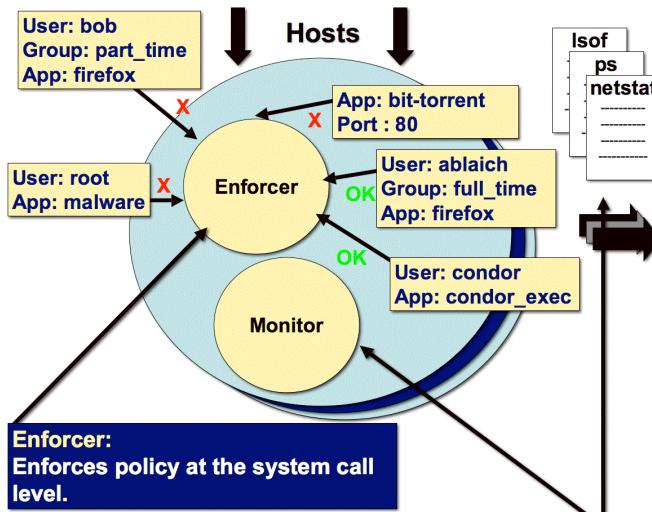
Andrew Blaich, Qi Liao,
Greg Allan, Brian Sullivan,
Aaron Striegel,
Douglas Thain
<http://netscale.cse.nd.edu/>

Higher-Level Policy:

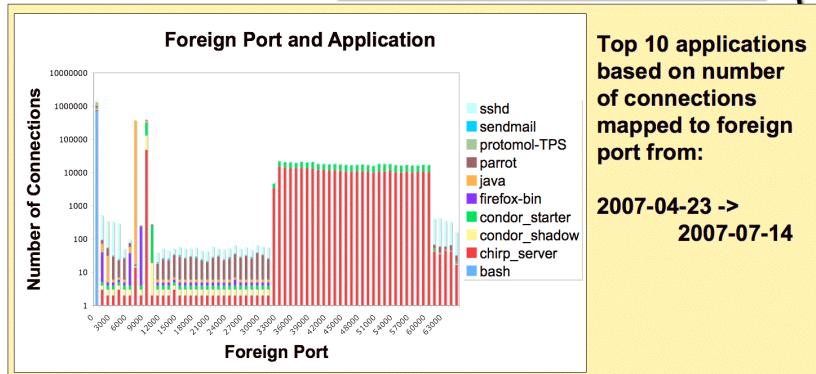
- Deny part-time employees from browsing the web.
- Allow full time employees to browse the web only using firefox.
- Allow condor-based grid jobs access to the network.
- Allow users to remote login throughout the network.
- Deny all other network activity.

Lower-Level Policy:

```
[allow/deny,machine,port,application,user/group,protocol]
allow,*,*,firefox,*,full_time,*
allow,*,*,condor_*,condor,*,*
allow,*,22,sshd,*,*,*
deny,*,*,*,*,*,*
```



Data Distribution:



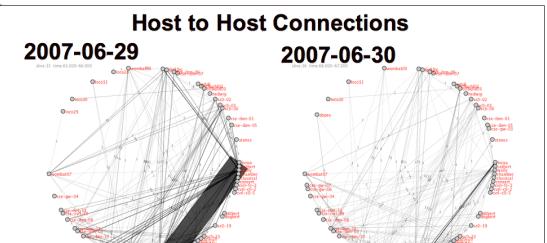
Synopsis:

Traditional network security tools enforce a policy based on host addresses and port numbers. However, hosts and ports are often not sufficient to define a strong security policy. The Lockdown system allows a network security officer to define, distribute, and enforce a security policy that takes into account local context (such as username and application) in addition to hosts and ports. System activity is collected in a central database for monitoring and analysis.

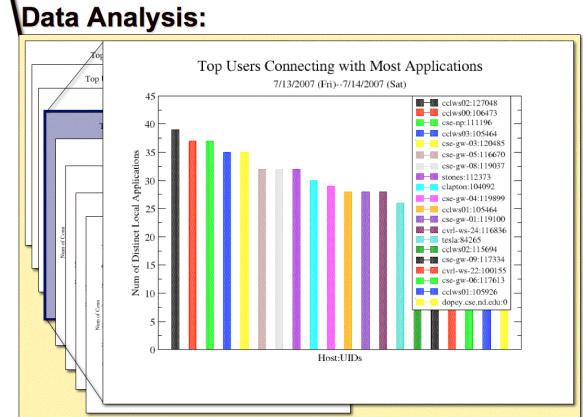
Local Context:

User	Connection Type	Count
Node: condor-07	Network Connection made by User condor	35772
Node: condor-10	Network Connection made by User condor	33099
Node: condor-20	Network Connection made by User condor	25972
Node: condor-40	Network Connection made by User condor	25871
Node: condor-60	Network Connection made by User condor	25871
Node: condor-80	Network Connection made by User condor	25871
Node: condor-100	Network Connection made by User condor	25871
Node: condor-120	Network Connection made by User condor	25871
Node: condor-140	Network Connection made by User condor	25871
Node: condor-160	Network Connection made by User condor	25871
Node: condor-180	Network Connection made by User condor	25871
Node: condor-200	Network Connection made by User condor	25871
Node: condor-220	Network Connection made by User condor	25871
Node: condor-240	Network Connection made by User condor	25871
Node: condor-260	Network Connection made by User condor	25871
Node: condor-280	Network Connection made by User condor	25871
Node: condor-300	Network Connection made by User condor	25871
Node: condor-320	Network Connection made by User condor	25871
Node: condor-340	Network Connection made by User condor	25871
Node: condor-360	Network Connection made by User condor	25871
Node: condor-380	Network Connection made by User condor	25871
Node: condor-400	Network Connection made by User condor	25871
Node: condor-420	Network Connection made by User condor	25871
Node: condor-440	Network Connection made by User condor	25871
Node: condor-460	Network Connection made by User condor	25871
Node: condor-480	Network Connection made by User condor	25871
Node: condor-500	Network Connection made by User condor	25871
Node: condor-520	Network Connection made by User condor	25871
Node: condor-540	Network Connection made by User condor	25871
Node: condor-560	Network Connection made by User condor	25871
Node: condor-580	Network Connection made by User condor	25871
Node: condor-600	Network Connection made by User condor	25871
Node: condor-620	Network Connection made by User condor	25871
Node: condor-640	Network Connection made by User condor	25871
Node: condor-660	Network Connection made by User condor	25871
Node: condor-680	Network Connection made by User condor	25871
Node: condor-700	Network Connection made by User condor	25871
Node: condor-720	Network Connection made by User condor	25871
Node: condor-740	Network Connection made by User condor	25871
Node: condor-760	Network Connection made by User condor	25871
Node: condor-780	Network Connection made by User condor	25871
Node: condor-800	Network Connection made by User condor	25871
Node: condor-820	Network Connection made by User condor	25871
Node: condor-840	Network Connection made by User condor	25871
Node: condor-860	Network Connection made by User condor	25871
Node: condor-880	Network Connection made by User condor	25871
Node: condor-900	Network Connection made by User condor	25871
Node: condor-920	Network Connection made by User condor	25871
Node: condor-940	Network Connection made by User condor	25871
Node: condor-960	Network Connection made by User condor	25871
Node: condor-980	Network Connection made by User condor	25871
Node: condor-1000	Network Connection made by User condor	25871
Node: condor-1020	Network Connection made by User condor	25871
Node: condor-1040	Network Connection made by User condor	25871
Node: condor-1060	Network Connection made by User condor	25871
Node: condor-1080	Network Connection made by User condor	25871
Node: condor-1100	Network Connection made by User condor	25871
Node: condor-1120	Network Connection made by User condor	25871
Node: condor-1140	Network Connection made by User condor	25871
Node: condor-1160	Network Connection made by User condor	25871
Node: condor-1180	Network Connection made by User condor	25871
Node: condor-1200	Network Connection made by User condor	25871
Node: condor-1220	Network Connection made by User condor	25871
Node: condor-1240	Network Connection made by User condor	25871
Node: condor-1260	Network Connection made by User condor	25871
Node: condor-1280	Network Connection made by User condor	25871
Node: condor-1300	Network Connection made by User condor	25871
Node: condor-1320	Network Connection made by User condor	25871
Node: condor-1340	Network Connection made by User condor	25871
Node: condor-1360	Network Connection made by User condor	25871
Node: condor-1380	Network Connection made by User condor	25871
Node: condor-1400	Network Connection made by User condor	25871
Node: condor-1420	Network Connection made by User condor	25871
Node: condor-1440	Network Connection made by User condor	25871
Node: condor-1460	Network Connection made by User condor	25871
Node: condor-1480	Network Connection made by User condor	25871
Node: condor-1500	Network Connection made by User condor	25871
Node: condor-1520	Network Connection made by User condor	25871
Node: condor-1540	Network Connection made by User condor	25871
Node: condor-1560	Network Connection made by User condor	25871
Node: condor-1580	Network Connection made by User condor	25871
Node: condor-1600	Network Connection made by User condor	25871
Node: condor-1620	Network Connection made by User condor	25871
Node: condor-1640	Network Connection made by User condor	25871
Node: condor-1660	Network Connection made by User condor	25871
Node: condor-1680	Network Connection made by User condor	25871
Node: condor-1700	Network Connection made by User condor	25871
Node: condor-1720	Network Connection made by User condor	25871
Node: condor-1740	Network Connection made by User condor	25871
Node: condor-1760	Network Connection made by User condor	25871
Node: condor-1780	Network Connection made by User condor	25871
Node: condor-1800	Network Connection made by User condor	25871
Node: condor-1820	Network Connection made by User condor	25871
Node: condor-1840	Network Connection made by User condor	25871
Node: condor-1860	Network Connection made by User condor	25871
Node: condor-1880	Network Connection made by User condor	25871
Node: condor-1900	Network Connection made by User condor	25871
Node: condor-1920	Network Connection made by User condor	25871
Node: condor-1940	Network Connection made by User condor	25871
Node: condor-1960	Network Connection made by User condor	25871
Node: condor-1980	Network Connection made by User condor	25871
Node: condor-2000	Network Connection made by User condor	25871
Node: condor-2020	Network Connection made by User condor	25871
Node: condor-2040	Network Connection made by User condor	25871
Node: condor-2060	Network Connection made by User condor	25871
Node: condor-2080	Network Connection made by User condor	25871
Node: condor-2100	Network Connection made by User condor	25871
Node: condor-2120	Network Connection made by User condor	25871
Node: condor-2140	Network Connection made by User condor	25871
Node: condor-2160	Network Connection made by User condor	25871
Node: condor-2180	Network Connection made by User condor	25871
Node: condor-2200	Network Connection made by User condor	25871
Node: condor-2220	Network Connection made by User condor	25871
Node: condor-2240	Network Connection made by User condor	25871
Node: condor-2260	Network Connection made by User condor	25871
Node: condor-2280	Network Connection made by User condor	25871
Node: condor-2300	Network Connection made by User condor	25871
Node: condor-2320	Network Connection made by User condor	25871
Node: condor-2340	Network Connection made by User condor	25871
Node: condor-2360	Network Connection made by User condor	25871
Node: condor-2380	Network Connection made by User condor	25871
Node: condor-2400	Network Connection made by User condor	25871
Node: condor-2420	Network Connection made by User condor	25871
Node: condor-2440	Network Connection made by User condor	25871
Node: condor-2460	Network Connection made by User condor	25871
Node: condor-2480	Network Connection made by User condor	25871
Node: condor-2500	Network Connection made by User condor	25871
Node: condor-2520	Network Connection made by User condor	25871
Node: condor-2540	Network Connection made by User condor	25871
Node: condor-2560	Network Connection made by User condor	25871
Node: condor-2580	Network Connection made by User condor	25871
Node: condor-2600	Network Connection made by User condor	25871
Node: condor-2620	Network Connection made by User condor	25871
Node: condor-2640	Network Connection made by User condor	25871
Node: condor-2660	Network Connection made by User condor	25871
Node: condor-2680	Network Connection made by User condor	25871
Node: condor-2700	Network Connection made by User condor	25871
Node: condor-2720	Network Connection made by User condor	25871
Node: condor-2740	Network Connection made by User condor	25871
Node: condor-2760	Network Connection made by User condor	25871
Node: condor-2780	Network Connection made by User condor	25871
Node: condor-2800	Network Connection made by User condor	25871
Node: condor-2820	Network Connection made by User condor	25871
Node: condor-2840	Network Connection made by User condor	25871
Node: condor-2860	Network Connection made by User condor	25871
Node: condor-2880	Network Connection made by User condor	25871
Node: condor-2900	Network Connection made by User condor	25871
Node: condor-2920	Network Connection made by User condor	25871
Node: condor-2940	Network Connection made by User condor	25871
Node: condor-2960	Network Connection made by User condor	25871
Node: condor-2980	Network Connection made by User condor	25871
Node: condor-3000	Network Connection made by User condor	25871

Network Visualization:



Data Analysis:



Presented at USENIX Security '07 Poster Session, August 2007
This work is supported by NSF Grant CNS-05-49087

